INTESI GROUP S.p.A.

Modello di organizzazione gestione e controllo ai sensi del Decreto Legislativo 231/01 – Parte Generale

Vers. 01

Data: 26 – 05 - 2026

COPYRIGHT DISCLAIMER

Tutti i Contenuti (testi, immagini, specifiche tecniche e altro) del presente documento sono **proprietà esclusiva e riservata di Intesi Group** e/o dei suoi aventi causa e/o di terzi soggetti ove indicati, e sono protetti dalle vigenti norme nazionali ed internazionali in materia di proprietà Intellettuale e/o Industriale.
É pertanto vietato utilizzare in qualsiasi modalità (a mero titolo esemplificativo, modificare, copiare, riprodurre, distribuire, trasmettere o diffondere) i suddetti Contenuti senza la previa autorizzazione scritta da parte del Titolare e/o dagli aventi diritto che se ne riservano espressamente ogni forma di riproduzione ed utilizzo. Ogni violazione sarà perseguita a norma di legge.

All Contents (texts, images, technical specifications and more) of this document are the **exclusive and reserved property of Intesi Group** and/or its successors in title and/or third parties where indicated, and are protected by current national and international regulations in intellectual and/or industrial property matters.
It is therefore forbidden to use in any way (by way of example only, modify, copy, reproduce, distribute, transmit or disseminate) the aforementioned Contents without the prior written authorization of the Owner and/or those entitled who expressly reserve any form of reproduction and use it. Any violation will be prosecuted according to the law.

Sommario

1. Descrizione del quadro normativo 5

2. Modello di Organizzazione, Gestione e Controllo e metodologia seguita per la sua predisposizione 19

3. L'Organismo di Vigilanza ai sensi del D.lgs. 231/01 25

4. Descrizione della realtà aziendale: elementi del modello di governance e dell'assetto organizzativo generale di Intesi Group S.p.A. 40

5. Sistema disciplinare 41

6. La diffusione del Modello 48

7. Adozione del Modello e criteri di aggiornamento ed adeguamento 49

8. Allegato - Elenco Reati D.lgs. 231/01 51

9. Sezione II - Parte speciale 67

10. Scopo 67

11. Analisi dei rischi – Approccio e metodo 69

12. Ambiente generale di controllo 79

13. Divieti di carattere generale 92

14. Le fattispecie di reato richiamate dal D.lgs. 231/2001 94

15. Le attività sensibili ai fini del D.lgs. 231/2001 97

16. Il sistema dei controlli 99

17. Descrizione schema tabelle 100

1. Descrizione del quadro normativo

1.1 Introduzione

In data 8 giugno 2001 è stato emanato - in esecuzione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300 - il Decreto Legislativo n. 231 (dal titolo "Disciplina della responsabilità amministrativa delle persone giuridiche e delle società e delle associazioni anche prive di personalità giuridica"), che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali cui l'Italia aveva già da tempo aderito.

Tale decreto ha introdotto la nuova disciplina della responsabilità amministrativa dell'Ente collettivo (dotato o meno di personalità giuridica) per taluni reati commessi nel proprio interesse o a proprio vantaggio da soggetti (e loro sottoposti) che ne esercitino (di diritto o di fatto) funzioni di rappresentanza, amministrazione e direzione.

Il legislatore ha pertanto inteso introdurre una responsabilità personale ed autonoma dell'Ente (di seguito anche "Società"), distinguendola da quella della persona fisica autore materiale del reato, in forza della quale l'Ente stesso risponde delle conseguenze del fatto illecito con il proprio patrimonio. Secondo la disciplina introdotta dal D.lgs. 231/01, infatti, le società possono essere ritenute "responsabili" per alcuni reati commessi o tentati, nell'interesse o a vantaggio delle società stesse, da esponenti dei vertici aziendali (i c.d. soggetti "in posizione apicale" o semplicemente "apicali") e da coloro che sono sottoposti alla direzione o vigilanza di questi ultimi (art. 5, comma 1, del D.lgs. 231/01).

Tale responsabilità amministrativa delle società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e si affianca a quest'ultima.

La finalità della normativa in questione è sostanzialmente quella di contrastare quei fenomeni di criminalità che si annidano dietro lo schermo della personalità giuridica.

Il D.lgs. 231/01 innova così l'ordinamento giuridico italiano in quanto alle società sono ora applicabili, in via diretta ed autonoma, sanzioni di natura sia pecuniaria che interdittiva in relazione a reati ascritti a soggetti funzionalmente legati alla società ai sensi dell'art. 5 del D.lgs. 231/01.

La responsabilità amministrativa della società è, tuttavia, esclusa se

I. la società prova:
   a) di aver adottato ed efficacemente attuato, prima della commissione dei reati, Modelli di Organizzazione, Gestione e Controllo idonei a prevenire i reati stessi;
   b) che il compito di vigilare sul funzionamento e l'osservanza dei modelli, di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo ("Organismo di Vigilanza");
   c) che le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
   d) non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di cui alla lettera b);
II. I soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi.

1.2 Natura della responsabilità

Con riferimento alla natura della responsabilità amministrativa ai sensi del D.lgs. 231/01, sono state prospettate in dottrina e in giurisprudenza varie impostazioni. Secondo una prima impostazione si tratta di responsabilità di natura amministrativa; secondo una seconda impostazione si tratta di responsabilità di natura penale, secondo una terza impostazione si tratta di un terzo genere di responsabilità.

Si può concludere che il D.lgs. 231/01 ha introdotto una forma di responsabilità delle società di tipo "amministrativo" ma con numerosi punti di contatto con una responsabilità di tipo "penale".

Sono di seguito elencate alcune norme che avvalorano quanto sopra rappresentato:

- l'art. 2 del D.lgs. 231/01, che ribadisce il principio di legalità tipico del diritto penale;
- l'art. 8 del D.lgs. 231/01, che prevede l'autonomia della responsabilità dell'ente rispetto all'accertamento della responsabilità della persona fisica autrice della condotta criminosa;
- l'art. 34 del D.lgs. 231/01, che stabilisce l'applicazione delle garanzie proprie del processo penale anche al procedimento relativo agli illeciti amministrativi dipendenti da reato;
- gli art. 9 e seguenti del D.lgs. 231/01, che precisano il carattere punitivo delle sanzioni applicabili alla società.

1.3 Autori del reato: soggetti in posizione apicale e soggetti sottoposti all'altrui direzione

Come sopra anticipato, secondo il D.lgs. 231/01, la società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da "persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente stesso" (sopra definiti soggetti "in posizione apicale" o "apicali"; art. 5, comma 1, lett. a), del D.lgs. 231/01);
- da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (i c.d. soggetti sottoposti all'altrui direzione; art. 5, comma 1, lett. b), del D.lgs. 231/01).

Sul punto, è comunque opportuno ribadire che la società non risponde, per espressa previsione legislativa (art. 5, comma 2, del D.lgs. 231/01), se le persone sopra indicate hanno agito nell'interesse esclusivo proprio o di terzi.

1.4 Le fattispecie di reato previste nel D.lgs. 231/01

La conoscenza dei reati, alla cui commissione da parte di soggetti qualificati ex art. 5 D.lgs. 231/01 è collegato il regime della responsabilità a carico dell'Ente, è quindi funzionale alla previsione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto. In particolare, i reati contemplati nella disciplina in oggetto sono riassumibili in differenti tipologie riportate nell'allegato alla presente parte generale.

1.5 Sistema sanzionatorio

Gli artt. 9 - 23 del D.lgs. 231/01 prevedono a carico della società, in conseguenza della commissione o della tentata commissione dei reati sopra menzionati, le seguenti sanzioni:

- sanzioni pecuniarie (e sequestro conservativo in sede cautelare);
- sanzioni interdittive (applicabili anche quali misure cautelari) di durata non inferiore a tre mesi e non superiore a due anni (salvo quanto indicato nell'articolo 25, comma 51 del D.lgs. 231/01 e salvi i casi di applicazione definitiva di seguito indicati), quali:
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
  - esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
  - divieto di pubblicizzare beni o servizi;
- confisca (e sequestro preventivo in sede cautelare);
- pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

[1] Art. 25, comma 5 D.lgs. 231/01, nei casi di condanna per uno dei delitti indicati nei commi 2 e 3 dell'articolo 25, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a quattro anni e non superiore a sette anni, se il reato e' stato commesso da uno dei soggetti di cui all'articolo 5, comma 1, lettera a), e per una durata non inferiore a due anni e non superiore a quattro, se il reato e' stato commesso da uno dei soggetti di cui all'articolo 5, comma 1, lettera b).

Quanto alle sanzioni pecuniarie, esse vengono determinate dal giudice penale attraverso un sistema basato su “quote” (in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di euro 258,22 a un massimo di euro 1.549,37 per quota).

In relazione alla commissione dei reati previsti dal Testo Unico Ambiente (D.lgs. n. 152/2006) si applicano, all’Ente sanzioni pecuniarie, da un minimo di centocinquanta quote ad un massimo di mille.

Oltre alle sanzioni pecuniarie sono applicate sanzioni interdittive previste dall’art. 9, comma 2, del D.lgs. 231/01, per una durata non inferiore a tre mesi e non superiore a due anni.

Nella commisurazione della sanzione pecuniaria, il giudice dovrà quindi indicare:

- il numero delle quote, tenendo conto della gravità del fatto, del grado di responsabilità della società, nonché dell’attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- l’importo della singola quota, sulla base delle condizioni economiche e patrimoniali della società.

Ai sensi dell’art. 12 comma 2, D.lgs. 231/01, le sanzioni pecuniarie vengono ridotte da un terzo alla metà, se prima della dichiarazione di apertura del dibattimento di primo grado:

- l’ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- ha adottato e reso operativo il Modello.

Nel caso in cui ricorrano entrambe le condizioni sopracitate, la sanzione è ridotta dalla metà ai due terzi.

Le sanzioni interdittive, invece, si applicano solo in relazione ai reati per i quali siano espressamente previste (si tratta, tra gli altri, dei reati contro la pubblica amministrazione, di taluni reati contro la fede pubblica, dei delitti in materia di terrorismo e di eversione dell’ordine democratico, dei delitti

contro la personalità individuale, dei reati in materia di sicurezza e salute sul lavoro, nonché dei reati transnazionali), e purché ricorra almeno una delle seguenti condizioni:

- la società deve aver ottenuto dalla consumazione del reato un profitto di rilevante entità ed il reato deve essere stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in tale ultimo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Il giudice determina il tipo e la durata della sanzione interdittiva tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso e, se necessario, può applicarle congiuntamente (art. 14, comma 1 e comma 3, D.lgs. 231/01).

Le sanzioni dell'interdizione dall'esercizio dell'attività, del divieto di contrattare con la pubblica amministrazione e del divieto di pubblicizzare beni o servizi possono essere applicate - nei casi più gravi (ai sensi dell'art. 16 del D.lgs. 231/01) - in via definitiva. È fatta salva la possibilità che il giudice conceda (in luogo dell'irrogazione della sanzione interdittiva che determina l'interruzione dell'attività) la prosecuzione dell'attività da parte di un commissario, ai sensi e alle condizioni di cui all'art. 15 del D.lgs. 231/01.

Il D.lgs. n. 121/2011 ha previsto anche l'applicazione dell'interdizione definitiva dall'esercizio dell'attività, ma solo nell'ipotesi in cui l'Ente o una sua attività organizzativa vengano stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione di alcuni reati (citati nel predetto D.lgs. n. 121/2011).

1.6 Delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti sanzionati sulla base del D.lgs. 231/01, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di durata) sono ridotte da un terzo alla metà.

La sanzioni non si applicano nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 D.lgs. 231/01): tale esclusione di sanzioni si giustifica in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e conto.

1.7 Vicende modificative dell'ente

Il D.lgs. 231/01 (artt. 28-33) si occupa altresì di disciplinare il regime della responsabilità patrimoniale dell'ente anche in relazione alle vicende modificative dello stesso, quali la trasformazione, la fusione, la scissione e la cessione d'azienda.

Il Legislatore ha, infatti, ritenuto opportuno trovare un equo contemperamento tra due diverse esigenze contrapposte, ovvero:

- da un lato, quella di evitare che tali operazioni possano costituire uno strumento per eludere agevolmente la responsabilità amministrativa dell'ente;
- dall'altro, quella di non penalizzare interventi di riorganizzazione privi di intenti elusivi.

In caso di trasformazione, quindi, l'art. 28 del D.lgs. 231/01 prevede (in coerenza con la natura di tale istituto, che implica un semplice mutamento del tipo sociale, senza determinare l'estinzione del soggetto giuridico originario) che resta ferma la responsabilità dell'ente per i reati commessi anteriormente alla data in cui la trasformazione abbia avuto effetto.

In caso di fusione, invece, l'ente che risulta dalla fusione (anche per incorporazione) e che, pertanto, assume tutti i diritti e gli obblighi delle società partecipanti all'operazione (art. 2504-bis, primo comma, Codice civile) risponderà dei reati di cui erano responsabili gli enti partecipanti alla fusione (art. 29 del D.lgs. 231/01).

In caso di scissione, infine, l'art. 30 del D.lgs. 231/01 prevede che:

- nel caso di scissione parziale, resta ferma la responsabilità dell'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto (fatto salvo quanto indicato all'ultimo paragrafo, art. 30, comma 3, D.Lgs 231/01);
- gli enti beneficiari della scissione (sia totale che parziale) siano solidalmente obbligati al pagamento delle sanzioni pecuniarie dovute dall'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto, nel limite del valore effettivo del patrimonio netto trasferito al singolo ente. Tale limite non si applica alle società beneficiarie, alle quali risulta devoluto, anche solo in parte, il ramo di attività nel cui ambito è stato commesso il reato.

Le sanzioni interdittive relative ai reati commessi anteriormente alla data in cui la scissione ha avuto effetto si applicano agli enti cui è rimasto o è stato trasferito, anche in parte, il ramo di attività nell'ambito del quale il reato è stato commesso (art. 30, comma 3, D.Lgs 231/01).

L'art. 31 del D.lgs. 231/01 prevede disposizioni comuni alla fusione e alla scissione, concernenti la determinazione delle sanzioni nell'eventualità che tali operazioni straordinarie siano intervenute prima della conclusione del giudizio. Viene chiarito, in particolare, il principio per cui il giudice deve commisurare la sanzione pecuniaria, secondo i criteri previsti dall'art. 11, comma 2, del D.lgs. 231 del 2001, facendo riferimento in ogni caso alle condizioni economiche e patrimoniali dell'ente originariamente responsabile.

In caso di sanzione interdittiva, l'ente risultante dalla fusione e l'ente al quale, nel caso di scissione, è applicabile la sanzione interdittiva possono chiedere al giudice la conversione della sanzione interdittiva in sanzione pecuniaria, a patto che:

- la carenza organizzativa che abbia reso possibile la commissione del reato sia stata eliminata (cfr. art 17, comma 1, lettera b), D.lgs. 231/01); e
- l'ente abbia provveduto a risarcire integralmente il danno e messo a disposizione (per la confisca) la parte di profitto eventualmente conseguito (cfr. art 17, comma 1, lettere a) e c), D.lgs. 231/01).

In caso di cessione (o di conferimento) dell'azienda nella cui attività è stato commesso il reato, è infine previsto (art. 33 del D.lgs. 231/01) che il cessionario sia solidalmente obbligato al pagamento della sanzione pecuniaria comminata al cedente, con le seguenti limitazioni:

- è fatto salvo il beneficio della preventiva escussione del cedente;
- la responsabilità del cessionario è limitata al valore dell'azienda ceduta e alle sanzioni pecuniarie che risultano dai libri contabili obbligatori ovvero dovute per illeciti amministrativi dei quali era, comunque, a conoscenza.

Al contrario, le sanzioni interdittive inflitte al cedente non sembrano estendersi al cessionario.

1.8 Reati Commessi all'estero

Si noti che, in forza del D.lgs. 231/01, l'ente può inoltre essere considerato responsabile, in Italia, per la commissione all'estero di taluni reati. In particolare, l'art. 4 del D.lgs. 231/01 prevede che gli enti aventi la sede principale nel territorio dello Stato rispondano anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del Codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Pertanto, l'ente è perseguibile quando:

- in Italia ha la sede principale2. In relazione alle imprese soggette alla iscrizione nel registro delle imprese che svolgono attività commerciale, gli artt. 2196 e 2197 del Codice civile impongono l'obbligo di indicare la sede e in caso di più sedi, la sede principale e le sedi secondarie. In caso divergenza tra il dato formale e quello effettivo sarà rilevante la sede effettiva (ove si svolgono le attività amministrative e di direzione). Rispetto alle associazioni e alle società prive di personalità giuridica dovrà farsi riferimento alle indicazioni dello statuto o dell'atto costitutivo. In

[2] Il D.Lgs 231/01 non fornisce un'autonoma definizione di "sede principale": è, pertanto, necessario riferirsi ai criteri civilistici.

relazione alle persone giuridiche non commerciali rileva la sede effettiva (art. 46 Codice civile) (in tali casi oltre alla sede formale andrà verificata anche la sede in concreto);

- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;
- la richiesta del Ministro della Giustizia, cui sia eventualmente subordinata la punibilità, è riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità ex art. 6 del Codice penale, in forza del quale "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

1.9 Procedimento di accertamento dell'illecito

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale.

A tale proposito, l'art. 36 del D.lgs. 231/01 prevede "La competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai quali gli stessi dipendono.

Per il procedimento di accertamento dell'illecito amministrativo dell'ente si osservano le disposizioni sulla composizione del tribunale e le disposizioni processuali collegate relative ai reati dai quali l'illecito amministrativo dipende".

Altra regola, ispirata a ragioni di effettività, omogeneità ed economia processuale, è quella dell'obbligatoria riunione dei procedimenti: il procedimento nei confronti dell'ente dovrà essere riunito, per quanto possibile, al procedimento penale instaurato nei confronti della persona fisica autore del reato presupposto della responsabilità dell'ente (art. 38 del D.lgs. 231/01).

Tale regola trova, tuttavia, un contemperamento nel dettato dell'art. 38, comma 2, del D.lgs. 231/01, che disciplina i casi specifici in cui si procede separatamente per l'illecito amministrativo.

1.10 L'adozione del Modello organizzativo di gestione quale condizione esimente dalla responsabilità amministrativa

Il D.lgs. 231/01 prevede agli artt. 6 e 7 condizioni specifiche per l'esonero dell'Ente dalla responsabilità, distinguendo il caso del reato commesso da soggetti in posizione apicale dal caso del reato commesso da loro sottoposti, precisando che per soggetti in posizione apicale si intendono coloro i quali, pur prescindendo dall'attività nominativamente svolta, rivestono funzioni di rappresentanza, amministrazione o direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché quei soggetti che, anche di fatto, esercitano la gestione e il controllo dell'Ente (membri del consiglio di amministrazione o del comitato esecutivo, direttori generali, etc.).

Nell'ipotesi di reati commessi da soggetti in posizione apicale, l'Ente non può essere quindi ritenuto responsabile qualora dimostri che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione e di Gestione idoneo a prevenire reati della specie di quello verificatosi;
- l'organo dirigente abbia affidato il compito di vigilare sul funzionamento, l'osservanza e l'aggiornamento del Modello ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo;
- gli autori del reato hanno commesso il reato eludendo fraudolentemente il Modello di Organizzazione e Gestione adottato;
- non vi è stata insufficiente o omessa vigilanza da parte dell'organismo deputato al controllo.

La società dovrà, dunque, dimostrare la sua estraneità ai fatti contestati al soggetto apicale, provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di conseguenza, la circostanza che la commissione del reato non deriva da una propria "colpa organizzativa".

In merito ai reati commessi da soggetti sottoposti all'altrui direzione, i soggetti presi in considerazione sono coloro i quali, pur se dotati di autonomia (pertanto, passibili di incorrere in illeciti), sono sottoposti alla direzione ed alla vigilanza dei soggetti apicali. Nella categoria devono essere inclusi anche i lavoratori c.d. parasubordinati, legati all'Ente da rapporti di collaborazione e, pertanto, sottoposti ad una più o meno intensa attività di vigilanza e direzione da parte dell'Ente stesso.

Nell'ipotesi di reati commessi da sottoposti, l'Ente è ritenuto responsabile qualora l'illecito sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza.

In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché' al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

L'art. 7, comma 4, del D.lgs. 231/01 si preoccupa di definire anche i requisiti per considerare efficace l'attuazione dei Modelli Organizzativi.

Precisamente:

- una verifica periodica ed un'eventuale modifica del Modello, quando vengano scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione e nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Da quanto sopra si evince che, nell'ipotesi di reati commessi da sottoposti, l'onere di provare la mancata adozione e l'inefficace attuazione del Modello graverà sull'accusa.

In estrema sintesi, in ipotesi di giudizio, la responsabilità dell'Ente si presume, qualora il reato sia stato commesso da soggetti in posizione apicale, mentre l'onere della prova spetta al PM od alla Parte Civile nel caso di reati commessi da sottoposti.

Il Decreto in esame prevede, peraltro, che il Modello di Organizzazione e Gestione da adottare quale condizione esimente risponda a determinati requisiti, modulati in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati riscontrabile nel contesto di riferimento.

Tali requisiti si traducono di fatto nella costruzione di un Modello atto a:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi reati della fattispecie prevista dal D.lgs. 231/01;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

1.11 Codici di comportamento predisposti dalle associazioni rappresentative degli enti

L'art. 6, comma 3, del D.lgs. 231/01 prevede "I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di

concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati".

Sul punto, Confindustria ha definito le "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.lgs. n. 231/01", aggiornate, da ultimo, nel giugno 2021 (di seguito, "Linee guida di Confindustria"), fornendo, tra l'altro, indicazioni metodologiche per l'individuazione delle aree di rischio (settore/attività nel cui ambito possono essere commessi reati), la progettazione di un sistema di controllo (i c.d. protocolli per la programmazione della formazione ed attuazione delle decisioni dell'ente) e i contenuti del Modello di Organizzazione, Gestione e Controllo.

Intesi Group S.p.A. ha adottato il proprio Modello di Organizzazione, Gestione e Controllo sulla base delle Linee guida di Confindustria, di cui si riportano in sintesi i punti fondamentali:

- individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei reati;
- predisposizione di un sistema di controllo e gestione in grado di prevenire i rischi attraverso l'adozione di apposite procedure. Le componenti del sistema di controllo devono essere ispirate ai seguenti principi:
  - verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
  - applicazione del principio di separazione delle funzioni;
  - documentazione dei controlli;
  - previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice di Condotta e delle procedure previste dal Modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, in termini di autonomia e indipendenza; professionalità; continuità di azione; onorabilità e assenza di conflitti di interesse, al fine di evitare che a tale organo siano attribuiti compiti operativi che ne comprometterebbero l'obiettività di giudizio;
- individuazione delle caratteristiche dell'Organismo di Vigilanza (composizione mono o plurisoggettiva, funzione, poteri…) e dei relativi obblighi di informazione.

1.12 Idoneità del Modello Organizzativo

L'accertamento della responsabilità della società (attribuito al giudice penale) comporta la verifica del fatto che il reato presupposto sia stato commesso e l'idoneità del Modello organizzativo adottato a prevenire la commissione del reato (si applica il criterio della c.d. "prognosi postuma").

Il giudizio di idoneità verrà, infatti, formulato ex ante, dovendo il giudice collocarsi idealmente nella realtà aziendale al momento in cui si è verificato l'illecito per valutare la congruenza e l'affidabilità del Modello adottato.

In particolare, sarà quindi considerato "idoneo a prevenire i reati" il Modello Organizzativo che, prima della commissione del reato, fosse in grado di eliminare o quantomeno di ridurre, con un grado di ragionevole certezza, il rischio della commissione del reato (successivamente verificatosi).

2. Modello di Organizzazione, Gestione e Controllo e metodologia seguita per la sua predisposizione

2.1 Descrizione

Intesi Group S.p.A., sensibile all'esigenza di assicurare condizioni di correttezza e di trasparenza nello svolgimento delle proprie attività, a tutela dell'immagine e della posizione propria e delle società del gruppo cui appartiene, a tutela dei propri soci, dipendenti e terzi correlati, ha ritenuto di procedere, alla redazione ed adozione del Modello di organizzazione e di gestione come previsto dal Decreto Legislativo 231/01.

L'adozione di un Modello di organizzazione, gestione e controllo a norma del D.lgs. 231/01 e la sua efficace e costante attuazione, oltre a rappresentare un motivo di esenzione dalla responsabilità di Intesi Group S.p.A. con riferimento alla commissione di alcune tipologie di reato, è infatti un atto di responsabilità sociale di Intesi Group S.p.A. da cui scaturiscono benefici per soci, dipendenti, creditori e per tutti gli altri soggetti i cui interessi sono legati alle sorti dell'azienda.

Tale iniziativa è stata presa nella convinzione che l'adozione di tale Modello e la sua revisione possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano nell'ambito di Intesi Group S.p.A. affinché gli stessi seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel D.lgs. 231/01.

L'introduzione di un sistema di controllo dell'attività imprenditoriale, unitamente alla fissazione e divulgazione di principi etici, migliorando i già elevati standard di comportamento adottati da Intesi Group S.p.A., aumenta la fiducia e la reputazione di cui Intesi Group S.p.A. gode nei confronti dei soggetti terzi e, soprattutto, assolve una funzione normativa, in quanto regola comportamenti e decisioni di coloro che quotidianamente sono chiamati a operare in favore di Intesi Group S.p.A. in conformità ai suddetti principi etici.

Intesi Group S.p.A. ha, quindi, inteso avviare una serie di attività volte a costruire e rendere il proprio Modello organizzativo conforme ai requisiti previsti dal D.lgs. 231/01 e coerente con i principi già radicati nella propria cultura di governo.

A fronte di quanto sopra, per maggiore chiarezza, si ritiene quindi opportuno esporre le metodologie seguite e i criteri adottati nelle varie fasi del progetto per la revisione del Modello.

2.2 Funzioni del Modello

Lo scopo del Modello Organizzativo adottato è sostanzialmente identificabile nella costruzione di un sistema strutturato ed organico di procedure ed attività di controllo volto a prevenire i reati di cui al D.lgs. 231/01: pertanto, ai fini di una corretta costruzione dello stesso, appare fondamentale la preventiva individuazione delle attività esposte a rischio di reato e la loro conseguente strutturazione procedurale.

Quale corollario di tale assunto vengono attribuite al Modello le seguenti funzioni primarie:

- determinare, in tutti coloro che operano in nome e per conto di Intesi Group S.p.A., la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni;
- ribadire che ogni forma di comportamento illecito è fortemente condannata in quanto contraria, oltre che a specifiche disposizioni di legge, ai principi etico-sociali cui Intesi Group S.p.A. intende uniformarsi nell'espletamento della propria missione;
- dotare Intesi Group S.p.A. di strumenti di monitoraggio sulle "aree di attività a rischio", a fini di un'adeguata e tempestiva azione di prevenzione e contrasto nella commissione dei reati stessi.

L'architettura di un simile Modello deve prevedere pertanto:

- le regole di comportamento cui uniformarsi;
- l'individuazione (c.d. mappatura) delle "aree di attività a rischio", intendendo con tale termine le attività in cui si ritiene esistano maggiori possibilità di commissione dei reati, in considerazione anche della specifica attività svolta da Intesi Group S.p.A., che di per sé esclude alcuni ambiti e ne evidenzia altri.

Costituiscono esempi di "attività sensibili", in linea generale, tutte quelle aree di attività aziendali nell'ambito o nell'esercizio delle quali è astrattamente ipotizzabile che sia commesso uno dei reati presupposto (ad esempio, che il reato di lesioni colpose sia commesso ove ci sia una realtà produttiva o stabilimento o che il rischio del reato di corruzione possa essere configurato ove vi siano rapporti con la PA). Accanto a questa valutazione che è appunto teorica, ne viene svolta una pratica in relazione alle specifiche aree di attività aziendale, analizzate partitamente per tramite dello strumento delle interviste ai soggetti apicali e operativi delle rispettive funzioni. Tali soggetti, rispondendo ai quesiti posti circa le modalità di funzionamento della specifica area ed alle procedure di compliance e funzionamento in essere, oltre che fornendo la necessaria documentazione (ove presente), forniscono un quadro completo delle regole di funzionamento dell'attività.

Questi principi regolatori dell'area di rischio sono poi partitamente analizzati sia sotto il profilo strettamente penale, che sotto i diversi profili pertinenti alle rispettive professionalità che hanno

contribuito alla redazione del Modello (giuslavoristico, regolamentare e societario, fiscale e tributario, privacy, antiriciclaggio e sicurezza sul lavoro) per addivenire ad una quantificazione, su scala, del rischio che effettivamente Intesi Group S.p.A. possa essere attinta da un'imputazione ex D.lgs. 231/01 per fatto di un proprio soggetto apicale o sottoposto al controllo, per fatti commessi nell'interesse o vantaggio della stessa.

Venendo allo specifico, nel caso di Intesi Group S.p.A., come meglio si vedrà nella parte speciale, si tratta di una Società adeguatamente proceduralizzata. Le procedure sono per la quasi totalità connotate da controlli incrociati e sono aggiornate periodicamente.

Quelle più sensibili sono gestite con l'ausilio di soggetti con specifiche competenze e ciò rende, quantomeno al livello di valutazione ex ante richiesta per l'espletamento di codesta valutazione, complessivamente ridotto il rischio de quo.

Si rimanda sul punto alla parte speciale per singole valutazioni.

2.3 Il progetto di Intesi Group S.p.A. per la definizione del proprio Modello di organizzazione, gestione e controllo a norma del D.lgs. 231/01

L'art. 6, comma 2, lett. a) del D.lgs. 231/01 indica, innanzitutto, tra i requisiti del Modello, l'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati espressamente richiamati dal decreto stesso. Si tratta, in altri termini, di quelle attività e processi aziendali che comunemente vengono definiti "sensibili" (di seguito, "Attività Sensibili" e "Processi Sensibili").

A seguire, sono stati identificati i soggetti aziendali che, in base a funzioni e responsabilità, hanno una conoscenza approfondita delle aree sensibili, nonché dei meccanismi di controllo in essere.

Intesi Group S.p.A. ha effettuato un'indagine dei fattori di rischio e degli elementi di criticità tipici del suo agire, considerando il suo grado di complessità aziendale, le competenze presenti, i processi decisionali attuati e la c.d. procedimentalizzazione dell'attività.

In questa fase assumono un ruolo importante l'analisi dei flussi informativi aziendali (le comunicazioni) e dei flussi decisionali, nonché la politica attuata da Intesi Group S.p.A. (intesa sia come concreta distribuzione del potere che come analisi dei rapporti di forza esistenti tra le diverse unità).

La valutazione del grado di rischio, cui è esposta Intesi Group S.p.A., è stata effettuata in sede di mappatura delle attività aziendali, con riguardo a ciascuna attività sensibile e processo strumentale, sulla base di considerazioni di tipo quantitativo e qualitativo che hanno tenuto conto, a titolo esemplificativo, dei seguenti fattori: frequenza dell'accadimento, dell'evento o dell'attività e gravità delle sanzioni potenzialmente associabili alla commissione di uno dei reati.

Si è provveduto quindi a verificare – per ogni area aziendale – la possibilità della commissione dei singoli reati presupposto della responsabilità amministrativa ex D.lgs. 231/01.

È stato quindi verificato il sistema di controllo esistente ed è stato, infine, predisposto il Modello di Organizzazione, Gestione e Controllo di Intesi Group S.p.A., che rappresenta un insieme coerente di principi, regole e disposizioni che:

- incidono sul funzionamento interno di Intesi Group S.p.A. e sulle modalità con le quali la stessa si rapporta con l'esterno;
- regolano la diligente gestione di un sistema di controllo delle attività sensibili, finalizzato a prevenire la commissione, o la tentata commissione, dei reati richiamati dal D.lgs. 231/01;
- assicurano condizioni di trasparenza e correttezza nella conduzione delle attività aziendali a tutela della reputazione e dell'immagine, proprie e delle società controllate, degli interessi degli azionisti e del lavoro dei propri dipendenti;

- mirano a prevenire i reati che potrebbero essere posti in essere sia da parte di soggetti apicali sia da parte dei loro sottoposti, e a dare luogo all'esonero da responsabilità dell'ente in caso di commissione di uno dei reati individuati nel D.lgs. 231/01.

Il presente documento è costituito da una "Parte Generale", che contiene i principi cardine del Modello, e da una "Parte Speciale", predisposta in considerazione delle singole attività aziendali, dei processi sensibili rilevati e delle procedure applicabili, per evitare il compimento delle diverse categorie di reato contemplate nel D.lgs. 231/01.

È stato quindi preliminarmente necessario identificare gli ambiti aziendali, oggetto dell'intervento, i processi e le attività sensibili.

2.4 Concetto di rischio accettabile

Un concetto critico da tener presente nella costruzione di qualunque Modello organizzativo, gestionale e di controllo è quello di "rischio accettabile".

Pertanto, anche ai fini dell'applicazione delle norme del D.lgs. 231/01 assume importanza la definizione di una soglia che permetta di porre un limite alla quantità e qualità degli strumenti di prevenzione da introdurre al fine di inibire la commissione del reato.

In relazione al rischio di commissione dei reati di cui D.lgs. 231/01, la soglia di accettabilità deve essere tale da consentire la costruzione di un sistema preventivo che non possa essere aggirato, se non fraudolentemente, violando quindi intenzionalmente il Modello Organizzativo adottato.

Nella redazione del Modello si è associato ad ogni area oggetto di analisi una valutazione del rischio corruttivo insito nell'attività svolta, necessario al fine di una attenta individuazione delle più corrette procedure di prevenzione e per una più efficace attuazione.

Quindi, per le sue caratteristiche, un sistema di controllo preventivo efficace deve essere in grado di:

- escludere che un qualunque soggetto operante all'interno di Intesi Group S.p.A. possa giustificare la propria condotta adducendo l'ignoranza delle direttive aziendali;
- evitare che, nella normalità dei casi, il reato possa essere causato dall'errore umano, dovuto anche a negligenza o imperizia, nella valutazione delle direttive aziendali.

3. L'Organismo di Vigilanza ai sensi del D.lgs. 231/01

In base alle previsioni del D.lgs. 231/01 – art. 6, comma 1, lett. a) e b) – l'Ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 del D.lgs. 231/01, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

I requisiti principali dell'Organismo di Vigilanza, così come proposti dalle Linee guida per la predisposizione dei Modelli di Organizzazione e Gestione emanate da Confindustria e fatti propri anche dagli organi giudicanti nelle diverse pronunce giurisprudenziali pubblicate, possono essere così identificati:

- autonomia;
- indipendenza;
- professionalità;
- continuità di azione
- disponibilità dei mezzi organizzativi e finanziari necessari per lo svolgimento delle proprie funzioni.

Il D.lgs. 231/01 non fornisce indicazioni specifiche circa la composizione dell'Organismo di Vigilanza (di seguito, anche "O.d.V.").

Il Consiglio di Amministrazione di Intesi Group S.p.A. ha optato per una composizione collegiale dell'Organismo di Vigilanza.

L'Organismo di Vigilanza con particolare riguardo ai profili di tutela della salute e sicurezza sul lavoro, dovrà avvalersi di tutte le risorse che Intesi Group S.p.A. ha attivato per la gestione dei relativi aspetti (RSPP - Responsabile del Servizio di Prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC – Medico Competente, addetti primo soccorso, addetto emergenze in caso d'incendio).

3.1 Principi generali in tema di istituzione, nomina e revoca dell'Organismo di Vigilanza

In attuazione di quanto previsto dall'art. 6 del D.lgs. 231/01, è quindi istituito presso Intesi Group S.p.A. l'Organismo di Vigilanza, al quale, in forza di autonomi poteri di iniziativa e controllo, sono stati assegnati i compiti di vigilanza dell'applicazione e di aggiornamento del Modello.

Tenuto conto della peculiarità delle sue attribuzioni e dei contenuti professionali specifici da esse richieste, nello svolgimento dei compiti di vigilanza e controllo, l'Organismo di Vigilanza sarà coadiuvato dalle singole funzioni aziendali e potrà essere supportato da uno staff dedicato (selezionato, anche a tempo parziale, per compiti specifici).

L'Organismo di Vigilanza di Intesi Group S.p.A. ha come principali referenti il Consiglio di Amministrazione e, qualora necessario, il Collegio Sindacale e altri profili professionali di diversi settori, ai quali dovrà riferire l'eventuale commissione dei reati e le eventuali carenze del Modello.

In ottemperanza a quanto stabilito dall'art. 6, comma 1, lett. b) del D.lgs. 231/01, secondo cui l'Organismo di Vigilanza è dotato di "autonomi poteri di iniziativa e controllo" e alla luce delle indicazioni fornite dalle Linee Guida di Confindustria, Intesi Group S.p.A. si riserva di determinare la composizione e le competenze professionali dell'Organismo di Vigilanza contestualmente all'atto di nomina.

L'Organismo di Vigilanza è nominato dal C.d.A.

L'adozione del Modello Organizzativo così come l'insediamento dell'O.d.V. sono efficaci contestualmente alla data di scrittura di specifico verbale nei libri sociali.

Sarà comunque sempre necessario che i componenti dell'Organismo di Vigilanza possiedano, oltre a competenze professionali adeguate, requisiti soggettivi che garantiscano l'autonomia, l'indipendenza e l'onorabilità richiesta dal compito.

In particolare, non possono essere nominati quali componenti dell'Organismo di Vigilanza:

- coloro che versano in una delle cause di ineleggibilità o di decadenza previste dall'art. 2382 Codice civile per gli amministratori;
- coloro che sono imputati per uno dei reati di cui al D.lgs. 231/01;
- coloro che sono stati condannati alla reclusione a seguito di processo penale avente ad oggetto la commissione di un delitto;
- il coniuge, i parenti e gli affini entro il quarto grado dei consiglieri della Società e delle società da questa controllate e/o controllanti, partecipate e/o partecipanti.

Qualora venissero a mancare uno o più componenti dell'Organismo di Vigilanza, il Consiglio di Amministrazione provvederà alla sostituzione con propria deliberazione.

L'incarico potrà altresì essere revocato da Intesi Group S.p.A., ma solo a fronte di uno dei seguenti motivi:

- gravi e accertati motivi di incompatibilità che ne vanifichino indipendenza e autonomia;
- grave negligenza nell'espletamento dei compiti connessi all'incarico;
- violazione degli obblighi di riservatezza previsti a carico dell'Organismo di Vigilanza;
- cessazione, accertata dal Consiglio di Amministrazione, dalla carica di responsabile della funzione ricoperta, qualora la nomina all'Organismo di Vigilanza sia stata legata al ruolo di responsabile di tale funzione aziendale. In ogni caso, qualsiasi

provvedimento di disposizione di carattere organizzativo che riguardi il responsabile della funzione (ad es. spostamenti ad altro incarico, licenziamenti, provvedimenti disciplinari, nomina di nuovo responsabile) dovrà essere deliberato dal Consiglio di Amministrazione.

La revoca dell'Organismo di Vigilanza o di un suo membro compete al Consiglio di Amministrazione. La delibera di revoca deve essere assunta con la maggioranza dei consensi dei consiglieri presenti con diritto di voto.

Il Consiglio di Amministrazione nella riunione nella quale delibera la revoca di un membro dell'Organismo di Vigilanza provvederà anche alla sua sostituzione.

3.2 Funzioni e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono conferiti i poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del D.lgs. 231/01.

Pertanto, a tale Organismo è affidato il compito di vigilare in generale:

- sulla reale (e non meramente formale) efficacia del Modello e sulla sua adeguatezza rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il D.lgs. 231/01;
- sull'osservanza delle prescrizioni del Modello da parte dei destinatari;
- sull'aggiornamento del Modello nel caso in cui si riscontrassero esigenze di adeguamento in relazione alle mutate condizioni aziendali o normative.

A tal fine, all'Organismo di Vigilanza è garantito libero accesso – presso tutte le funzioni della Società, senza necessità di alcun consenso preventivo – a ogni informazione, dato o documento aziendale ritenuto rilevante per lo svolgimento dei propri compiti e deve essere costantemente informato dal management: a) sugli aspetti dell'attività aziendale che possono esporre la Società al rischio di

commissione di uno dei reati; b) sui rapporti con i consulenti e con i partner che operano per conto della società nell'ambito di operazioni sensibili; c) sulle operazioni straordinarie della Società.

L'Organismo di Vigilanza è tenuto al vincolo di riservatezza rispetto a tutte le informazioni di cui è a conoscenza a causa dello svolgimento del suo incarico.

La divulgazione di tali informazioni potrà essere effettuata solo ai soggetti e con le modalità previste dal Modello.

3.3 Reporting dell'Organismo di Vigilanza verso il vertice aziendale

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

L'Organismo di Vigilanza ha due linee di reporting:

- la prima, in caso di criticità, direttamente verso l'Amministratore Delegato;
- la seconda nei confronti del Consiglio di Amministrazione e del Collegio Sindacale, riportando almeno semestralmente l'attività svolta (controlli effettuati e esito degli stessi, le verifiche specifiche e l'esito delle stesse, l'eventuale aggiornamento della mappatura dei Processi Sensibili, ecc.).

Qualora l'Organismo di Vigilanza rilevi criticità riferibili a qualcuno dei membri del Consiglio di Amministrazione o del Collegio Sindacale, la corrispondente segnalazione è da destinarsi prontamente a uno degli altri soggetti non coinvolti.

Gli incontri con gli organi cui l'Organismo di Vigilanza riferisce devono essere verbalizzati e copie dei verbali devono essere custodite dall'Organismo di Vigilanza e/o dagli organi di volta in volta coinvolti.

Il Collegio Sindacale, il Consiglio di Amministrazione e l'Amministratore Delegato hanno la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

3.4 Flussi informativi verso l'Organismo di Vigilanza

L'Organismo di Vigilanza nell'ambito dei suoi poteri di iniziativa e controllo riceve dalle funzioni aziendali competenti le informazioni necessarie all'espletamento del suo compito di vigilanza sul funzionamento e l'osservanza del Modello nonché del suo aggiornamento.

In particolare, l'Organismo di Vigilanza deve essere informato senza ritardo relativamente a:

- infortuni gravi o gravissimi (infortunio che ha determinato una prima prognosi uguale o superiore ai 40 giorni, un ricovero ospedaliero, un indebolimento permanente di un senso o di un organo);
- per quanto attiene i rapporti con Enti Pubblici (Agenzia delle Entrate, Ispettorato del Lavoro, INPS, INAIL, ARPA, ASL, ecc.), rilievi e sanzioni comminate da essi a fronte di verifiche ispettive.

Inoltre, l'organismo di Vigilanza deve essere periodicamente informato:

- per quanto attiene la salute e sicurezza sui luoghi di lavoro in merito a:
  - riepilogo infortuni con assenza maggiore di 40 giorni e malattie professionali riconosciute;
  - informazioni relative ad infortuni accaduti;
  - situazione sorveglianza sanitaria;
  - riepilogo visite ispettive da parte di Enti Pubblici (INAIL, ASL, ecc.) (numero visite, motivazioni ed eventuali provvedimenti impartiti);
  - certificazione ISO 45001:2018: situazioni Audit annuali/triennali (ove applicabile);

- eventuali aggiornamenti del documento di valutazione dei rischi (revisioni e/o aggiornamenti) e del piano di emergenza;
- pianificazione/esecuzione delle prove di evacuazione;
- aggiornamento relativo alla formazione obbligatoria;
- analisi delle risultanze di eventuali audit condotti dalle funzioni interne preposte e stato avanzamento azioni correttive;
- aggiornamento dei procedimenti penali e civili;
- eventuali provvedimenti disciplinari;

- per quanto attiene la tutela dell'ambiente:
  - certificazione ISO 14001:2015: situazioni Audit annuali/triennali (ove applicabile);
  - riepilogo visite ispettive da parte di Enti Pubblici (ARPA, Province/Città Metropolitane/Regioni, ecc.) (numero visite, motivazioni e eventuali provvedimenti impartiti);
  - analisi delle risultanze di eventuali audit condotti dalle funzioni interne preposte e stato avanzamento azioni correttive;
  - aggiornamento dei procedimenti penali e civili in materia;
  - eventuali provvedimenti disciplinari;
  - stato avanzamento attività di bonifica/messa in sicurezza (ove applicabile).

Oltre alle segnalazioni di cui sopra, devono essere inoltre obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.lgs. 231/01 o dalla normativa in materia di salute e sicurezza sul lavoro e che possano coinvolgere Intesi Group S.p.A.;
- le richieste di assistenza legale inoltrate dal Presidente o dal Consiglio di Amministrazione o dipendenti in caso di avvio di procedimento giudiziario nei loro

confronti ed in relazione ai reati di cui al D.lgs. 231/01 o alla normativa in materia di salute e sicurezza sul lavoro;

- le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le comunicazioni inerenti modifiche organizzative e societarie;
- le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici erogazioni, contributi, sovvenzioni.

Tutte le segnalazioni e le comunicazioni indirizzate all'Organismo di Vigilanza di Intesi Group S.p.A. potranno essere inoltrate al seguente indirizzo e-mail: odv@intesigroup.com

3.5 Sistema di segnalazione delle violazioni (Whistleblowing)

I dipendenti, organi sociali, consulenti e partner sono tenuti a segnalare violazioni di condotte illecite, rilevanti ai sensi del D.lgs. 231/01, ovvero del Modello, di cui siano venuti a conoscenza.

Chiunque voglia effettuare una segnalazione potrà utilizzare uno dei canali indicati nel Codice di Condotta, disponibile sul sito intranet e Internet della Società.

La Procedura pubblicata nella pagina intranet adottata da Intesi Group S.p.A., stabilisce:

- Come effettuare una segnalazione relativa ad una violazione o condotta illecita
- le linee guida per gestire le Segnalazioni
- gli standard di protezione per i segnalanti, i facilitatori e le persone correlate.

La procedura garantisce i principi di riservatezza, protezione dell'anonimato e divieto di ritorsione, in conformità con le normative applicabili. Le disposizioni contenute non pregiudicano né limitano in alcun modo il diritto o l'obbligo, come eventualmente definiti dalla normativa applicabile, di segnalazione alle autorità regolamentari, di vigilanza o giudiziarie competenti nei Paesi dove opera la Società e/o a qualsiasi organo di controllo istituito presso la Società.

La procedura è redatta conformemente alle seguenti normative:

- D. Lgs. 231/01 recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica";
- D. Lgs. 24/23 recante "Attuazione della direttiva europea 1937/19 del Parlamento Europeo e del Consiglio, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali";
- Regolamento (UE) 2016/679, recante "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- D. Lgs 196/13 e s.m.i., recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.";

nonché al Modello di Organizzazione Gestione e Controllo, al Codice di Condotta e al sistema disciplinare adottati dalla Società ai sensi del D.lgs. 231/01.

Per "whistleblowing" si intende l'azione di segnalazione di violazioni da parte del segnalante.

Le segnalazioni devono fornire elementi utili a consentire ai soggetti preposti di procedere alle dovute e appropriate verifiche ed accertamenti (art. 6, comma 2-bis, D.lgs. 231/01).

Le "segnalazioni" forniscono informazioni su possibili violazioni. Le "violazioni" riguardano azioni od omissioni commesse durante le attività lavorative o collegate alle stesse, da qualsiasi soggetto all'interno della Società, per suo conto o nei rapporti con la Società o gli stakeholder della Società, che si sono verificate, si può ragionevolmente supporre che si siano verificate oppure che è molto probabile che si verifichino, così come tentativi di occultare tali azioni od omissioni, e che:

- costituiscano o possano costituire una violazione, o un'induzione ad una violazione oppure vanifichino l'oggetto o la finalità:
  - di leggi e altre normative applicabili, a tutti i livelli (internazionale, nazionale, regionale, locale), fatte salve eventuali limitazioni specifiche definite dalla normativa applicabile localmente (si veda il D. Lgs. 24/23, art. 1 "Ambito di applicazione oggettivo");
  - dei valori e dei principi stabiliti nel Codice di Condotta della Società e nelle altre procedure della Società in materia di anticorruzione;
  - del Modello di Organizzazione Gestione e Controllo, al Codice di Condotta e al sistema disciplinare adottati dalla Società ai sensi del D.lgs. 231/01, delle Policy e delle Procedure della Società e dei principi di controllo interno; e/o
- costituiscano o possano costituire illeciti amministrativi, contabili, civili o penali; e/o
- causino o possano causare qualsiasi tipo di danno (per esempio economico, ambientale, di sicurezza o reputazionale) alla Società, ai suoi dipendenti e a terzi, quali ad esempio, fornitori, clienti, partner commerciali o la comunità esterna; e/o
- siano identificate come pertinenti dalle normative applicabili che disciplinano la segnalazione di violazioni delle disposizioni normative.

I "destinatari" della Procedura Whistleblowing sono le persone fisiche che hanno ottenuto direttamente o indirettamente informazioni in merito a violazioni, a titolo esemplificativo e non esaustivo:

- dipendenti, inclusi ex dipendenti e candidati in fase di selezione;
- collaboratori (liberi professionisti, consulenti, volontari, stagisti, ecc.);
- membri degli organi sociali (inclusi i membri degli organi amministrativi, gestionali o di vigilanza) e azionisti della Società;
- dipendenti, collaboratori, membri degli organi sociali e azionisti, di clienti, fornitori, subfornitori (inclusa tutta la catena di approvvigionamento) e altri partner commerciali (comprese le joint-venture);

- qualsiasi terzo affiliato alle persone menzionate in precedenza;
- comunità locali e membri delle organizzazioni della società civile (per es. ONG);
- più in generale, qualsiasi stakeholder della Società.

Un "segnalante" è qualsiasi persona che presenti una segnalazione.

La "persona segnalata" è l'autore o il presunto autore della violazione.

Il "gestore delle segnalazioni" è la funzione Legal & Compliance o la/e persona/e incaricata/e di gestire la segnalazione ricevuta, in base ai canali di segnalazione stabiliti.

I "facilitatori" sono le persone fisiche che assistono un segnalante nella procedura di segnalazione, collegate a quest'ultimo da un legame lavorativo.

Le "persone correlate" sono persone fisiche che hanno una relazione personale o lavorativa con il segnalante.

Le estensioni o le limitazioni alla tutela legale garantita ai segnalanti e altre parti correlate/di supporto possono variare in base alle leggi applicabili localmente, al loro ruolo e al tipo di violazione segnalata.

La Società si impegna a rispettare i seguenti principi generali nella gestione del processo di whistleblowing e richiede che tutte le persone coinvolte li rispettino per quanto di competenza:

- Principio di riservatezza: la Società garantisce la riservatezza dei segnalanti, delle segnalazioni e delle informazioni contenute al loro interno, come meglio precisato al punto "riservatezza";
- Principio di proporzionalità: le indagini condotte dalla Società sono adeguate, necessarie e commisurate per raggiungere lo scopo delle stesse;
- Principio di imparzialità: l'analisi e il trattamento delle segnalazioni vengono eseguiti senza soggettività, indipendentemente dalle opinioni e dagli interessi delle persone responsabili della loro gestione;

- Principio di buona fede: le tutele al segnalante sono applicabili anche nei casi in cui la segnalazione si riveli infondata, qualora sia stata fatta in buona fede (ovvero il segnalante aveva motivi fondati di ritenere che le informazioni relative alle violazioni fossero vere al momento della segnalazione e che le informazioni rientrassero nell'ambito della Procedura); nessun segnalante può approfittare di tali tutele per evitare una sanzione disciplinare a proprio carico.

L'adozione e l'aggiornamento della Procedura Whistleblowing è responsabilità della funzione Legal & Compliance, previa consultazione delle rappresentanze e/o delle organizzazioni sindacali, ove presenti, in merito all'individuazione del canale di segnalazione interno o a sue modifiche. La Procedura Whistleblowing è pubblicata nella intranet aziendale nonché sul sito ufficiale dell'azienda.

Nella intranet e del sito web istituzionale sono pubblicate informazioni chiare sul canale, sulle procedure e sui presupposti per poter effettuare le segnalazioni interne o esterne nel caso in cui:

- la segnalazione interna non sia ancora stata valutata;
- la segnalazione interna non abbia avuto alcun seguito, non sia stata adeguatamente valutata o non sia stata adottata alcuna misura correttiva adeguata;
- il segnalante abbia fondati motivi di ritenere che ad un'eventuale segnalazione interna non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- il segnalante abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Nell'incoraggiare a segnalare tempestivamente qualsiasi violazione, la Società garantisce la riservatezza di ciascuna segnalazione e delle informazioni contenute al suo interno, ivi compresa l'identità del segnalante, della/e persona/e segnalata/e, dei facilitatori e di ogni altra persona coinvolta. Le loro identità non saranno comunicate a nessuno al di fuori del gestore delle segnalazioni, tranne:

- laddove forniscano il proprio consenso esplicito, oppure abbiano intenzionalmente divulgato la propria identità in altri ambiti;
- la comunicazione è un obbligo necessario e proporzionato nell'ambito di indagini da parte delle Autorità o di procedimenti giudiziari, ai sensi della normativa applicabile.

Le informazioni contenute nelle segnalazioni che costituiscono segreti commerciali non possono essere usate o divulgate per finalità diverse da quelle necessarie per risolvere la Segnalazione.

La Società non tollera alcuna forma di minaccia, ritorsione o discriminazione, tentata o effettiva, ai danni dei segnalanti, dei facilitatori, delle persone correlate, dalle persone segnalate e di chiunque abbia collaborato alle indagini per comprovare la fondatezza della segnalazione.

La Società si riserva il diritto di intraprendere azioni adeguate contro chiunque attui, o minacci di porre in essere, atti di ritorsione contro i soggetti elencati in precedenza, fatto salvo il diritto delle parti coinvolte di tutelarsi legalmente qualora siano state riscontrate responsabilità di natura penale o civile legate alla falsità di quanto dichiarato o segnalato.

Coerentemente con quanto stabilito dal Codice di Condotta, nessuno può essere de-mansionato, licenziato, sospeso, minacciato, molestato, soggetto ad intimidazioni a seguito di una segnalazione effettuata in buona fede.

Chiunque realizzi ritorsioni contro chi abbia segnalato in buona fede o effettui una segnalazione intenzionalmente falsa ed infondata sarà sottoposto a procedimenti disciplinari che potrebbero anche comportare il licenziamento, coerentemente con quanto stabilito nel Codice di Condotta.

La Società può intraprendere le più opportune misure disciplinari e/o legali, nella misura consentita dalla normativa applicabile, a tutela dei propri diritti, dei propri beni e della propria immagine, nei confronti di chiunque abbia effettuato in mala fede segnalazioni false, infondate od opportunistiche e/o al solo scopo di calunniare, diffamare o arrecare pregiudizio alla persona segnalata o ad altre parti coinvolte nella segnalazione.

I dati personali (ivi inclusi eventuali dati appartenenti a categorie particolari, quali l'origine razziale ed etnica, le convinzioni religiose e filosofiche, le opinioni politiche, l'adesione a partiti politici o sindacati, nonché i dati personali idonei a rivelare lo stato di salute e l'orientamento sessuale, dati relativi a eventuali reati o condanne penali) dei segnalanti e di altri soggetti eventualmente coinvolti, acquisiti in occasione della gestione delle segnalazioni, saranno trattati per l'adempimento degli obblighi imposti dalla normativa applicabile sul "Whistleblowing", nei limiti e con le garanzie previste da tale normativa, in piena conformità a quanto stabilito dalle normative applicabili in materia di protezione dei dati personali.

Il trattamento dei dati personali sarà effettuato dal gestore delle segnalazioni (fatte salve eventuali specifiche normative locali in materia ed eventuali conflitti di interesse), ai soli fini di dare esecuzione alle procedure stabilite nella Procedura Whistleblowing.

Secondo i principi di "privacy by design" (protezione dei dati fin dalla progettazione) e "privacy by default and minimization" (privacy mediante impostazione predefinita e minimizzazione), la Società ha predisposto canali riservati per ricevere le segnalazioni e le gestisce in modo sicuro per garantire l'anonimato del segnalante oppure la riservatezza della sua identità e di qualsiasi terzo coinvolto (tranne per gli obblighi necessari e proporzionati nell'ambito di indagini da parte delle autorità competenti o di procedimenti giudiziari).

Il trattamento dei dati personali sarà limitato a quanto strettamente necessario e proporzionato per garantire la corretta gestione della segnalazione e comunque non oltre il termine previsto dalla normativa applicabile e da quanto definito nella Procedura Whistleblowing.

Le operazioni di trattamento dei dati sono affidate a dipendenti debitamente autorizzati, istruiti e specificamente formati in relazione all'esecuzione delle procedure di Whistleblowing, con particolare riferimento alle misure di sicurezza e alla tutela della riservatezza dei soggetti coinvolti e delle informazioni contenute nelle segnalazioni oppure a specialisti esterni, in questo caso adottando adeguate tutele contrattuali.

I dati personali contenuti nelle segnalazioni potranno essere comunicati dal gestore delle segnalazioni agli organi sociali e alle funzioni interne eventualmente di volta in volta competenti, così come all'Autorità Giudiziaria e/o a qualsiasi altra autorità competente, o a terze parti debitamente autorizzate, ai fini dell'attivazione delle procedure necessarie a garantire, in conseguenza della segnalazione, idonea tutela giudiziaria e/o disciplinare nei confronti della/e persona/e segnalata/e, laddove dagli elementi raccolti e dagli accertamenti effettuati emerga la fondatezza delle circostanze inizialmente segnalate.

L'esercizio dei diritti degli interessati previsti dalla normativa applicabile in materia di protezione dei dati personali potrà essere limitato ove necessario per garantire il pieno rispetto della normativa Whistleblowing applicabile e per tutelare la riservatezza delle segnalazioni e degli interessati.

L'Organismo di Vigilanza deve essere tempestivamente informato dalla funzione Legal & Compliance in merito alle segnalazioni rilevanti (relative a atti, comportamenti od eventi che possano determinare una violazione del Modello o che, più in generale, siano rilevanti ai fini del D.lgs. 231/01) e all'esito delle indagini.

Gli obblighi di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientrano nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 Codice civile.

Valgono, in proposito, le seguenti prescrizioni di carattere generale; devono essere raccolte eventuali segnalazioni relative:

- alla commissione, o al ragionevole pericolo di commissione, dei reati richiamati dal D.lgs. 231/01;
- la violazione di norme poste a tutela della salute e sicurezza sul lavoro;
- a "pratiche" non in linea con le norme di comportamento emanate dalla Società;
- a comportamenti che, in ogni caso, possono determinare una violazione del Modello.

4. Descrizione della realtà aziendale: elementi del modello di governance e dell'assetto organizzativo generale di Intesi Group S.p.A.

4.1 Intesi Group S.p.A.

Intesi Group S.p.A. ha per oggetto principale, sia in proprio che per conto terzi, l'analisi, la progettazione, la realizzazione, la verifica, la distribuzione, la manutenzione e l'assistenza in proprio e per conto di terzi, di programmi software e applicazioni WEB. Inoltre, ha come oggetto l'erogazione di servizi informatici e di certificazione, la produzione, l'assemblaggio e l'installazione di sistemi hardware; l'organizzazione, la gestione e la supervisione di procedure aziendali informatiche e banche dati, la progettazione, la produzione e la fornitura a privati, professionisti, aziende e enti pubblici, di siti internet, sistemi di commercio elettronico, portali, applicazioni di social network, WEB e mobile, sia in conto proprio che per conto terzi.

Si occupa, inoltre, di promozione, commercializzazione e installazione di prodotti software e servizi, sia in forma diretta che indiretta, anche mediante la locazione semplice o quella finanziaria da parte di terzi, la fornitura di SAAS (Software As A Service), la vendita per corrispondenza, per via telematiche con forme di franchising. Inoltre, la realizzazione di servizi di assistenza tecnica e manutenzione alla clientela, anche tramite la gestione di call center specializzati, sia in forma diretta che indiretta.

Informazioni di carattere generale:

Ragione sociale	Intesi Group S.p.A.
P.IVA	02780480964
Numero REA	MI - 1562415
Sede legale	Via Torino 48 – 20123 MILANO
Unità locali	nessuna
Sedi secondarie	nessuna

4.2 Modello di governance di Intesi Group S.p.A.

La società è amministrata da un Consiglio di Amministrazione composto da tre Amministratori il quale, allorquando non vi abbia provveduto l'assemblea, provvede altresì a nominare il Presidente conferendogli idonei poteri.

Il Consiglio di Amministrazione ha tutti i poteri di ordinaria e straordinaria amministrazione. La figura del Presidente coincide con quella dell'Amministratore Delegato, in quale ha ampi poteri gestori.

L'assemblea degli azionisti ha altresì nominato un Collegio Sindacale composto da 3 sindaci effettivi e 2 sindaci supplenti al quale è anche affidata la revisione contabile.

Le azioni ordinarie rappresentanti l'intero capitale della Società sono detenute da:

Dylog Italia Spa: 51%

Sironi Paolo: 49%.

5. Sistema disciplinare

5.1 Sistema disciplinare di Intesi Group S.p.A.

Aspetto essenziale per l'effettività del Modello 231 (ai sensi ai sensi dell'art. 6, comma 2, lettera e) del D.lgs. 231/01), così come del Codice di Condotta, è costituito dalla predisposizione di un adeguato sistema disciplinare, volto a sanzionare la violazione delle regole di condotta esposte nello stesso. Pertanto, la definizione di un adeguato sistema disciplinare costituisce un presupposto essenziale della valenza scriminante del Modello stesso.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.lgs. 231/01.

Si ricorda al riguardo (in sintesi):

- che la violazione dei doveri contenuti nel Codice di Condotta, compresi quelli relativi all'attuazione ed all'osservanza più in generale del Piano di Prevenzione della Corruzione e del Modello 231, è fonte di responsabilità disciplinare;
- che la violazione dei doveri è altresì rilevante ai fini della responsabilità civile, amministrativa e contabile ogni qualvolta le stesse responsabilità siano collegate alla violazione di doveri, obblighi, leggi o regolamenti.

Verificando le specifiche posizioni, si osserva quanto di seguito specificato, fermo restando l'eventuale richiesta di risarcimento degli eventuali danni causati a Intesi Group S.p.A. dai comportamenti posti in essere in violazione delle regole di cui al Modello, come nel caso di applicazione alla stessa da parte del Giudice delle misure cautelari previste dal D.lgs. 231/01.

5.2 Misure nei confronti di lavoratori subordinati

L'osservanza delle disposizioni e delle regole comportamentali previste dal Codice di Condotta e del Modello, come detto, costituisce adempimento da parte dei dipendenti degli obblighi previsti dall'art. 2104, comma secondo, c.c.

La violazione delle singole disposizioni e regole comportamentali in questione da parte dei dipendenti costituirà quindi sempre illecito disciplinare.

Le misure indicate nei documenti citati, il cui mancato rispetto si intende sanzionare, sono comunicate mediante circolare interna a tutti i dipendenti, sono affisse in luogo accessibile a tutti e sono vincolanti per tutti i dipendenti di Intesi Group S.p.A.

I provvedimenti disciplinari sono irrogabili nei confronti dei lavoratori dipendenti in conformità a quanto previsto dall'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori") ed eventuali normative speciali applicabili.

Alla notizia di una violazione del Modello e/o del Codice di Condotta, verrà quindi attivata la procedura di accertamento, in conformità al Contratto Collettivo Nazionale di Lavoro ("CCNL") applicabile allo specifico dipendente interessato dalla procedura.

Pertanto:

- a ogni notizia di violazione è dato impulso alla procedura di accertamento;
- nel caso in cui, a seguito della procedura, sia accertata una violazione, ad istanza dell'O.d.V., verrà individuata - analizzate le motivazioni del dipendente - la sanzione disciplinare applicabile in base al CCNL di riferimento;
- verrà così irrogata la sanzione disciplinare prevista dal CCNL applicabile e proporzionata alla gravità della violazione;
- verrà data informazione dell'irrogazione di tale sanzione all'O.d.V., che provvederà a verificare la concreta applicazione della stessa;
- laddove non si ritenga di dare corso alla segnalazione ricevuta da parte dell'O.d.V. e di irrogare conseguenti sanzioni, dovrà essere comunicato il motivato diniego scritto, giustificando le ragioni della propria scelta. Qualora l'O.d.V. non ritenga soddisfacenti le motivazioni addotte presenterà la questione, per la decisione, all'Organo Amministrativo.

5.2.1 Quadri e Impiegati

Sistema disciplinare

In conformità ai principi di tipicità delle violazioni e delle sanzioni, Intesi Group S.p.A. intende portare a conoscenza dei propri dipendenti le misure sanzionatorie applicabili, tenuto conto della gravità delle infrazioni.

Precisamente, i lavoratori sono passibili dei provvedimenti - nel rispetto delle procedure previste dall'articolo 7 della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili – previsti dall'apparato sanzionatorio del CCNL applicato da Intesi Group S.p.A., e precisamente:

- richiamo verbale;
- ammonizione scritta;
- multa;
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di 3 (tre) giorni;
- licenziamento.

Restano ferme - e si intendono qui richiamate – tutte le previsioni del CCNL, tra cui:

- l'obbligo – in relazione all'applicazione di qualunque provvedimento disciplinare – della previa contestazione dell'addebito al dipendente e dell'ascolto di quest'ultimo in ordine alla sua difesa;
- l'obbligo – salvo che per il richiamo verbale - che la contestazione sia fatta per iscritto e che il provvedimento non sia emanato se non decorsi 5 (cinque) giorni dalla contestazione dell'addebito (nel corso dei quali il dipendente potrà presentare le sue giustificazioni);
- l'obbligo di motivare al dipendente e comunicare per iscritto la comminazione del provvedimento.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, si procederà al conferimento di specifici poteri, nei limiti della rispettiva competenza, al management aziendale.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, e l'eventuale richiesta di risarcimento danni, sono applicate anche tenendo conto:

- dell'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia, con riguardo anche alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- delle mansioni del lavoratore;
- della posizione funzionale delle persone coinvolte nei fatti costituenti la violazione;
- delle altre particolari circostanze che accompagnano l'illecito disciplinare.

Violazione del Modello e relative sanzioni

Sono sanzionabili i seguenti comportamenti che costituiscono violazione del Modello:

- le violazioni, da parte del dipendente, di procedure interne previste dal Modello o l'adozione, nell'espletamento di attività connesse ai processi sensibili, di comportamenti non conformi alle prescrizioni del Modello sia che espongano sia che non espongano Intesi Group S.p.A. ad una situazione oggettiva di rischio di commissione di uno dei reati;
- l'adozione di comportamenti non conformi alle prescrizioni del Modello e diretti in modo univoco al compimento di uno o più reati;
- l'adozione di comportamenti in violazione delle prescrizioni del Modello, tale da determinare la concreta e/o potenziale applicazione a carico di Intesi Group S.p.A. di sanzioni previste dal D.lgs. 231/01.

5.2.2 Dirigenti

I comportamenti in violazione del Modello o l'adozione, nell'espletamento di attività connesse con i processi sensibili, di una condotta non conforme alle prescrizioni del Modello stesso, se commessi da dirigenti, possono far venir meno il rapporto fiduciario, con applicazione delle misure sanzionatorie più idonee, in conformità a quanto previsto dall'art. 2119 cod. civ. e dal contratto collettivo di lavoro applicabile per i dirigenti di azienda.

5.2.3 Misure nei confronti degli amministratori

In caso di comportamenti in violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Consiglio di Amministrazione ed il Collegio Sindacale, i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee consentite dalla legge.

5.2.4 Misure nei confronti dei sindaci

In caso di comportamenti in violazione del Modello da parte di uno o più sindaci, l'Organismo di Vigilanza informa l'intero Collegio Sindacale e il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

5.2.5 Misure nei confronti dei revisori

Alla notizia di violazione delle disposizioni e delle regole di comportamento del Modello da parte dei revisori, l'Organismo di Vigilanza dovrà tempestivamente informare dell'accaduto il Consiglio di Amministrazione.

I soggetti destinatari dell'informativa potranno così assumere, secondo quanto previsto dallo Statuto, gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci, al fine di adottare le misure più idonee previste dalla legge.

5.3 Misure nei confronti di partner commerciali, consulenti, collaboratori

Ogni violazione del Modello o del Codice di Condotta (sui temi inerenti alla corruzione) posta in essere da parte di collaboratori esterni o partner sarà invece sanzionata - secondo quanto previsto da specifiche clausole contrattuali inserite nei relativi contratti, lettere di incarico o accordi di partnership - con la risoluzione del rapporto contrattuale, fatte inoltre salve eventuali richieste di risarcimento qualora da tale comportamento derivino danni concreti a Intesi Group S.p.A.

5.4 Misure nei confronti dei sindaci

In caso di comportamenti in violazione del Modello da parte di uno o più sindaci, l'Organismo di Vigilanza informa l'intero Collegio Sindacale e il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

5.5 Misure nei confronti dei revisori

Alla notizia di violazione delle disposizioni e delle regole di comportamento del Modello da parte dei revisori, l'Organismo di Vigilanza dovrà tempestivamente informare dell'accaduto il Consiglio di Amministrazione.

I soggetti destinatari dell'informativa potranno così assumere, secondo quanto previsto dallo Statuto, gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci, al fine di adottare le misure più idonee previste dalla legge.

5.6 Misure nei confronti di partner commerciali, consulenti, collaboratori

Ogni violazione del Modello o del Codice di Condotta (sui temi inerenti alla corruzione) posta in essere da parte di collaboratori esterni o partner sarà invece sanzionata - secondo quanto previsto

da specifiche clausole contrattuali inserite nei relativi contratti, lettere di incarico o accordi di partnership - con la risoluzione del rapporto contrattuale, fatte inoltre salve eventuali richieste di risarcimento qualora da tale comportamento derivino danni concreti a Intesi Group S.p.A.

5.7 Misure nei confronti dei membri dell'Organismo di Vigilanza

Il sistema sanzionatorio di natura disciplinare e contrattuale come sopra individuato, troverà applicazione anche nei confronti dei membri dell'Organismo di Vigilanza.

6. La diffusione del Modello

La conoscenza del Modello è fondamentale per sviluppare la consapevolezza di tutti i destinatari che operino, per conto e/o nell'interesse della Società, nell'ambito dei processi sensibili di poter incorrere in illeciti passibili di conseguenze penalmente rilevanti, non solo per sé stessi ma anche per la Società, in caso di comportamenti contrari alle previsioni del D.lgs. 231/01 e al Modello.

Intesi Group S.p.A. deve garantire una corretta informazione/formazione sul contenuto del Modello, sia alle risorse già presenti in azienda sia a quelle da inserire, delle regole di condotta ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei Processi Sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza in collaborazione con il responsabile della funzione delegata a gestire le Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nella applicazione del Modello.

6.1 La comunicazione iniziale

L'adozione del Modello è comunicata a tutte le risorse presenti in azienda al momento dell'adozione stessa.

Ai nuovi assunti, invece, viene consegnato un set informativo (es. Codice di Condotta, CCNL, ecc.), con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

6.2 La formazione

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.lgs. 231/01 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società.

All'Organismo di Vigilanza è demandato altresì il controllo circa i contenuti dei programmi di formazione.

La partecipazione ai programmi di formazione è obbligatoria e il controllo circa l'effettiva frequenza è demandata all'Organismo di Vigilanza.

7. Adozione del Modello e criteri di aggiornamento ed adeguamento

7.1 Verifiche e controlli sul Modello

A seguito dell'approvazione e degli aggiornamenti del Modello, l'O.d.V. assume la funzione di responsabile per l'attuazione, da intendersi come attività strategica volta a favorirne l'effettiva osservanza.

Gli organismi di controllo dovranno, pertanto, preoccuparsi di predisporre annualmente il proprio programma di vigilanza, in cui verranno stabiliti e pianificati:

- un calendario delle attività da svolgere nel corso dell'anno;
- le cadenze temporali dei controlli;
- i criteri e le procedure di analisi;

- la possibilità di effettuare verifiche e controlli non programmati.

Gli organismi di controllo nello svolgimento della propria attività, potranno avvalersi sia del supporto di funzioni e strutture interne a Intesi Group S.p.A., con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo, sia di esperti esterni.

A tali organismi sono riconosciuti, nel corso delle verifiche e ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli.

7.2 Aggiornamento e adeguamento

Il Modello verrà adottato con delibera del Consiglio di Amministrazione che istituirà anche l'Organismo di Vigilanza. Ciascun membro del Consiglio di Amministrazione, così come il Collegio Sindacale della Società, si è impegnato al rispetto del Modello.

Il Modello è soggetto ad aggiornamenti ogniqualvolta siano introdotti nel D.lgs. 231/01 nuovi reati ritenuti potenzialmente applicabili alla Società od in caso di cambiamenti organizzativi, operativi e societari. Essendo il Modello un atto di emanazione dell'organo dirigente (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a) del D.lgs. 231/01) le modifiche e integrazioni sono di competenza del Consiglio di Amministrazione. Il Consiglio di Amministrazione può delegare specifiche modifiche all'Amministratore Delegato, fermo restando che dovrà ratificare annualmente le modifiche eventualmente apportate.

Rimane, in ogni caso, di esclusiva competenza del Consiglio di Amministrazione la delibera di aggiornamenti e/o di adeguamenti del documento dovuti ai seguenti fattori:

- intervento di modifiche normative;
- identificazione di nuove attività sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività d'impresa;
- commissione dei reati richiamati dalla Legge n. 190/2012 e dal D.lgs. n. 231/01 da parte dei destinatari;

- riscontro di carenze e/o lacune nelle previsioni del documento, a seguito di verifiche sull'efficacia del medesimo da parte degli organismi di controllo.

8. Allegato - Elenco Reati D.lgs. 231/01

Art. 24 - Indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o dell'unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture

Articolo modificato dalla L. 161/2017, dal D.lgs. n. 75/2020 e L. 137/2023:

- Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis Codice penale);
- Indebita percezione di erogazioni a danno dello stato (art.316-ter Codice penale);
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, Codice penale);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis Codice penale);
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter Codice penale);
- Frode nelle pubbliche forniture (art. 356 Codice penale);
- Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n. 898);
- Turbata libertà degli incanti (art. 353 c.p.);
- Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.).

Art. 24-bis - Delitti informatici e trattamento illecito di dati

Articolo aggiunto dalla L. 18 marzo 2008 n. 48 e successivamente modificato dai D.lgs. 07/2016, D.lgs. 08/2016 e dal D.L. 105/2019:

- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter Codice penale);
- Documenti informatici (art. 491-bis Codice penale);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater Codice penale);
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies Codice penale);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater Codice penale);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies Codice penale);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis Codice penale);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter Codice penale);
- Danneggiamento di sistemi informatici o telematici (art. 635-quater Codice penale);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies Codice penale);
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies Codice penale);
- Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica (art. 1 comma 11 D.L. 21 settembre 2019, n. 105 convertito con modificazioni dalla L. 18 novembre 2019, n. 133).

Art. 24-ter - Delitti di criminalità organizzata

Articolo aggiunto dalla L. n. 94/2009 e successivamente modificato dalla L. n. 69/2015:

- Associazione per delinquere (art. 416 Codice di Procedura Penale.);
- Associazione di tipo mafioso anche straniere (art. 416-bis Codice penale - articolo modificato dalla L. n. 69/2015);
- Scambio elettorale politico-mafioso (art. 416-ter Codice penale - articolo così sostituito dall´art. 1, comma 1, L. 21 maggio 2019);
- Sequestro di persona a scopo di estorsione (art. 630 Codice penale);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309, comma 7-bis aggiunto dal D.lgs. n. 202/2016);
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis Codice penale per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91);
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, comma 2, lett. a, numero 5, Codice di Procedura Penale).

Art. 25 - Peculato, concussione, induzione indebita a dare o promettere altre utilita' corruzione e abuso d'ufficio

Articolo modificato dalla L. n. 190/2012, dalla L. 3/2019 e dal D.lgs. n.75/2020:

- Concussione (art. 317 Codice penale) [articolo modificato dalla L. 69/2015 e dalla L. 161/2017];
- Corruzione per l'esercizio della funzione (art. 318 Codice penale) - modificato dalla L. 190/2012, dalla L. 69/2015 e dalla L. 3/2019;
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 Codice penale) - articolo modificato dalla L. 69/2015 e dalla L. 161/2017;
- Circostanze aggravanti (art. 319-bis Codice penale);
- Corruzione in atti giudiziari (art. 319-ter Codice penale) - articolo modificato dalla L. 69/2015 e dalla L. 161/2017;

- Induzione indebita a dare o promettere utilità (art. 319-quater Codice penale) - modificato dalla L. 190/2012, dalla L. 69/2015 e dalla L. 3/2019;
- Corruzione di persona incaricata di un pubblico servizio (art. 320 Codice penale);
- Pene per il corruttore (art. 321 Codice penale);
- Istigazione alla corruzione (art. 322 Codice penale);
- Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle comunità europee e di funzionari delle comunità europee e di stati esteri (art. 322 bis Codice penale) - modificato dalla L.n. 190/2012 e dalla L. n. 3/2019;
- Traffico di influenze illecite (art. 346-bis Codice penale) - modificato dalla L.3/2019;
- Peculato (limitatamente al primo comma) (art. 314 Codice penale) - introdotto dal D.lgs. n. 75/2020;
- Peculato mediante profitto dell'errore altrui (art. 316 Codice penale) - introdotto dal D.lgs. n. 75/2020;
- Abuso d'ufficio (art. 323 Codice penale) - introdotto dal D.lgs. n. 75/2020.

Art. 25-bis - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Articolo inserito dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001, successivamente modificato dalla L. n. 99/2009 e dal D.lgs. 125/2016:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 Codice penale);
- Alterazione di monete (art. 454 Codice penale);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 Codice penale);
- Spendita di monete falsificate ricevute in buona fede (art. 457 Codice penale);

- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 Codice penale);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 Codice penale);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 Codice penale);
- Uso di valori di bollo contraffatti o alterati (art. 464 Codice penale);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 Codice penale);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 Codice penale).

Art. 25-bis.1 - Delitti contro l'industria e il commercio

Articolo aggiunto dalla L. n. 99/2009:

- Turbata libertà dell'industria o del commercio (art. 513 Codice penale);
- Illecita concorrenza con minaccia o violenza" (art. 513-bis Codice penale);
- Frodi contro le industrie nazionali (art. 514);
- Frode nell'esercizio del commercio (art. 515 Codice penale);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 Codice penale);
- Vendita di prodotti industriali con segni mendaci (art. 517 Codice penale);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter Codice penale);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater Codice penale).

Art. 25-ter - Reati societari

Articolo aggiunto dal D.lgs. n. 61/2002, successivamente modificato dalle L. nn. 262/2005, 69/2015 ed infine dal D.lgs. 38/17:

- False comunicazioni sociali (art. 2621 Codice civile) - modificato dalla L.69/2015;
- Fatti di lieve entità (art. 2621-bis Codice civile);
- False comunicazioni sociali delle società quotate (art. 2622 Codice civile) - modificato dalla L.69/2015;
- Falso in prospetto (art. 173-bis D.lgs. 58/1998 che ha sostituito l'abrogato art. 2623 c.c.);
- Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale (art 27, D.lgs. 39/2010);
- Impedito controllo (art. 2625, comma 2, Codice civile);
- Indebita restituzione di conferimenti (art. 2626 Codice civile);
- Illegale ripartizione degli utili e delle riserve (art. 2627 Codice civile);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 Codice civile);
- Operazioni in pregiudizio dei creditori (art. 2629 Codice civile);
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis Codice civile);
- Formazione fittizia del capitale (art. 2632 Codice civile);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 Codice civile);
- Corruzione tra privati (art. 2635 Codice civile) - modificato dal D.lgs. 38/2017 e dalla L. 3/2019;
- Istigazione alla corruzione tra privati (art. 2635-bis Codice civile) - aggiunto dal D.lgs. 38/2017 e modificato dalla L. n. 3/2019;
- Illecita influenza sull'assemblea (art. 2636 Codice civile);
- Aggiotaggio (art. 2637 Codice civile);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 commi 1 e 2 Codice civile.).

Art. 25-quater - Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali

Articolo aggiunto dalla L. n. 7/2003:

- Associazioni sovversive (art. 270 Codice penale);
- Associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-bis Codice penale);
- Circostanze Aggravanti (art. 270 bis 1 Codice penale);
- Assistenza agli associati (art. 270-ter Codice penale);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270-quater Codice penale);
- Organizzazione di trasferimento per finalità di terrorismo (art. 270-quater1 Codice penale);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinqiues Codice penale);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinqiues1 Codice penale);
- Sottrazione di beni o denaro sottoposti a sequestro (art. 270- quinqiues2 Codice penale);
- Condotte con finalità di terrorismo (art. 270-sexies Codice penale);
- Attentato per finalità terroristiche o di eversione (art. 280 Codice penale);
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis Codice penale);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis Codice penale);
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 Codice penale);
- Cospirazione politica mediante accordo (art. 304 Codice penale);
- Cospirazione politica mediante associazione (art. 305 Codice penale);

- Banda armata: formazione e partecipazione (art. 306 Codice penale);
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 Codice penale);
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1);
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2);
- Atto di terrorismo nucleare (art. 280 ter Codice penale);
- Sequestro a scopo di coazione (art. 289-ter Codice penale) - introdotto dal D.lgs. 21/2018;
- Finanziamento di condotte con finalità di terrorismo (L. 153/2016);
- Sanzioni (L. 422/1989 art.3);
- Convenzione di New York del 9 dicembre 1999 (art.2).

Art. 25-quater.1 - Pratiche di mutilazione degli organi genitali femminili

Art. 583-bis Codice penale - articolo aggiunto dalla L. n. 07/2006

Art. 25-quinquies - Delitti contro la personalità individuale

Articolo aggiunto dalla L. n. 228/2003, successivamente modificato dalla L. n. 38/2006, dal D.lgs.n. 39/14, e dalla L. n. 199/2016:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 Codice penale);
- Prostituzione minorile (art. 600-bis Codice penale);
- Pornografia minorile (art. 600-ter Codice penale);
- Detenzione di materiale pornografico (art. 600-quater Codice penale);
- Pornografia virtuale (art. 600-quater.1 Codice penale);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies Codice penale);
- Tratta di persone (art. 601 Codice penale);
- Acquisto e alienazione di schiavi (art. 602 Codice penale);

- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis Codice penale);
- Adescamento di minorenni (art. 609 – undicies Codice penale).

Art. 25-sexies - Reati di abuso di mercato

Articolo aggiunto dalla L. n. 62/2005:

- Abuso di informazioni privilegiate (D.lgs. 24.02.1998, n. 58, art. 184);
- Manipolazione del mercato (D.lgs. 24.02.1998, n. 58, art. 185);
- Altre fattispecie in materia di abusi di mercato (Art. 187-quinques Testo Unico della Finanza) - articolo modificato dal D. Lgs. 107/2018.

Art. 25-septies - Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

Articolo aggiunto dalla L. n. 123/2007 e successivamente sostituito dall'Articolo 30 del D.Lgs 9 Aprile 2008 n 81:

- Omicidio colposo (art. 589 Codice penale);
- Lesioni personali colpose (art. 590 Codice penale)

Art. 25-octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Articolo aggiunto dal D.lgs. n. 231/2007 (come modificato tempo per tempo) e rubrica modificata dalla L. n. 186/2014:

- Ricettazione (art. 648 Codice penale)
- Riciclaggio (art. 648-bis Codice penale);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter Codice penale);

- Autoriciclaggio (art. 648-ter.1 Codice penale).

Art. 25 octies 1 - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

Articolo aggiunto dal D.lgs. n. 184 dell'8 novembre 2021, articolo 3, comma 1 e modificato dalla L. 137/2023:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter Codice penale)
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater Codice penale);
- Trasferimento fraudolento di valori (art. 512-bis c.p.).

Art. 25-novies - Delitti in materia di violazione del diritto d'autore

Articolo aggiunto dalla L. 23 luglio 2009 n. 99:

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, comma 1 lett a) bis, L. n. 633/1941);
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, comma 3, L. n. 633/1941);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis, comma 1, L. n. 633/1941);

- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis, comma 2, L. n. 633/1941);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter L. n. 633/1941);
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies L. n. 633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies L. n. 633/1941).

Art. 25-decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Art. 377-bis Codice penale - articolo aggiunto dall’art. 20 della L. 1° marzo 2001, n. 63.

Art. 25-undecies - Reati ambientali

Articolo aggiunto dalla D.lgs. n. 121/11 e successivamente modificato dalla L. n. 68/2015 e dal D.lgs. 21/2018:

- Inquinamento ambientale (art. 452-bis Codice penale);
- Disastro ambientale (art. 452-quarter Codice penale);
- Delitti colposi contro l'ambiente (art. 452- quinquies Codice penale);
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies Codice penale);
- Circostanze aggravanti (art. 452 – octies Codice penale);
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies Codice penale);
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari e di specie animali o vegetali selvatiche protette (art. 727-bis Codice penale);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis Codice penale);
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n. 150/1992, artt. 1, 2, 3-bis e 6);
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.lgs. 152/2006, art. 137);
- Attività di gestione di rifiuti non autorizzata (D.lgs. 152/2006, art. 256);
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.lgs. 152/2006, art. 257);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.lgs. 152/2006, art. 258);
- Traffico illecito di rifiuti (D.lgs. n. 152/2006, art. 259);

- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificate di analisi dei rifiuti; inserimento nel SISTRI di un certificate di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI – area movimentazione nel trasporto di rifiuti (D.lgs. 152/2006, art. 260-bis);
- Superamento dei valori limite di emissione (D.lgs. 152/2006, art. 279, comma 5)
- Inquinamento doloso provocato da navi (D.lgs. 202/2007, art.8);
- Inquinamento colposo provocato da navi (D.lgs. 202/2007, art. 9);
- Cessazione e riduzione dell'impiego di sostanze lesive (L. n. 549/1993, art.3).

Art. 25- duodecies - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Articolo aggiunto dal D.lgs. n. 109/2012 modificato dalla L. 161/2017:

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D.lgs. 286/1998);
- Disposizioni contro le immigrazioni clandestine (art.12 co.3, 3bis, 3ter e co. 5 D.lgs. 286/1998).

Art. 25-terdecies - Razzismo e xenofobia

- Art. 604 bis c.p.

Art. 25-quaterdecies - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati

Articolo inserito dall' art. 5, comma 1, L. 3 maggio 2019, n. 39, a decorrere dal 17 maggio 2019, ai sensi di quanto disposto dall' art. 7, comma 1, della medesima Legge n. 39/2019:

- Frode in competizioni sportive (art. 1 L. 401/1989);
- Esercizio abusivo di attività di gioco e scommessa (art. 4 L. 401/1989).

Art. 25-quinquiesdecies - Reati tributari

Articolo aggiunto dalla L. N. 157/2019 e dal D.lgs. N. 75/2020

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs. n. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D.lgs. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.lgs. 74/2000);
- Dichiarazione infedele (art. 4 D.lgs. n. 74/2000) - introdotto dal D.lgs. n. 75/2020;
- Omessa dichiarazione (art. 5 D.lgs. n. 74/2000) - introdotto dal D.lgs. n. 75/2020;
- Indebita compensazione (art. 10-quater D.lgs. n. 74/2000) - introdotto dal D.lgs. n. 75/2020.

Art. 25-sexiesdecies – Contrabbando

Articolo aggiunto dal D.lgs. n. 75/2020

- Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali (art. 282 DPR n. 43/1973);
- Contrabbando nel movimento delle merci nei laghi di confine (art. 283 DPR n. 43/1973);
- Contrabbando nel movimento marittimo delle merci (art. 284 DPR n. 43/1973);
- Contrabbando nel movimento delle merci per via aerea (art. 285 DPR n. 43/1973);
- Contrabbando nelle zone extra-doganali (art. 286 DPR n. 43/1973);
- Contrabbando per indebito uso di merci importate con agevolazioni doganali (art. 287 DPR n. 43/1973);
- Contrabbando nei depositi doganali (art. 288 DPR n. 43/1973);

- Contrabbando nel cabotaggio e nella circolazione (art. 289 DPR n. 43/1973);
- Contrabbando nell'esportazione di merci ammesse a restituzione di diritti (art. 290 DPR n. 43/1973);
- Contrabbando nell'importazione od esportazione temporanea (art. 291 DPR n. 43/1973);
- Contrabbando di tabacchi lavorati esteri (art. 291-bis DPR n. 43/1973);
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri (art. 291-ter DPR n. 43/1973);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater DPR n. 43/1973);
- Altri casi di contrabbando (art. 292 DPR n. 43/1973);
- Circostanze aggravanti del contrabbando (art. 295 DPR n. 43/1973).

Il mancato rispetto di procedure e/o disposizioni in tema di ambiente e sicurezza, rientra nel più ampio contesto delle sanzioni previste dal sistema disciplinare del "Modello 231" – Parte generale.

Art. 25-septiesdecies - Delitti contro il patrimonio culturale, Reati previsti dal nuovo titolo VIII-bis del Codice penale

Articolo aggiunto dall'art. 3, comma1, Legge 9 marzo 2022, n 22.

- furto di beni culturali (art. 518-bis c.p.);
- appropriazione indebita di beni culturali (art. 518-ter c.p.);
- ricettazione di beni culturali (art. 518-quater c.p.);
- falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.);
- violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.);
- importazione illecita di beni culturali (art. 518-decies c.p.);
- uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.);
- distruzione; dispersione, deterioramento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.);

- contraffazione di opere d'arte (art. 518-quaterdecies c.p.).

Art. 25-octiesdecies Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici

Articolo aggiunto dall'art. 3, comma1, Legge 9 marzo 2022, n 22.

- Riciclaggio di beni culturali (art. 518-sexies c.p.);
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.).

Reati transnazionali

Legge 16 marzo 2006, n. 146, artt. 3 e 10 - costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale:

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis Codice penale);
- Favoreggiamento personale (art. 378 Codice penale);
- Associazione per delinquere (art. 416 Codice penale);
- Associazione di tipo mafioso anche straniere (art. 416-bis Codice penale).

Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato – (Art. 12, L. n. 9/2013)

- Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473 Codice penale);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 Codice penale);
- Frode nell'esercizio del commercio (art. 515 Codice penale);
- Vendita di prodotti industriali con segni mendaci (art. 517 Codice penale).

Altre fattispecie in materia di abusi di mercato - (Art. 187- quinquies Testo Unico della Finanza - TUF) - modificato dal D.lgs. 107/2018

- divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 Reg. UE 596/2014);
- divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014).

9. Sezione II - Parte speciale

10. Scopo

La presente sezione ha la finalità di definire linee e principi di comportamento che devono essere osservati dai dipendenti, dai collaboratori e dagli esponenti aziendali di Intesi Group S.p.A. (anche "Società"), al fine di prevenire, nell'ambito delle specifiche attività svolte e considerate "a rischio", la commissione dei reati previsti dal D.lgs. 8 giugno 2001, n. 231 ("Decreto" o "D.lgs. 231/2001") e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la parte speciale del Modello ha lo scopo di:

- indicare le regole che i dipendenti, i collaboratori e gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutti i soggetti sopracitati dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello Organizzativo;
- Codice di Condotta;
- policies e procedure adottate dalla Società;
- dispense, materiale informativo e/o didattico sulla sicurezza sul lavoro;
- istruzioni operative;
- documento di valutazione dei rischi;
- incarichi e qualifiche operative;
- direttive aziendali;
- documentazione inerente le autorizzazioni, qualifiche, certificazioni, accreditamenti;
- procedura Whistleblowing;
- ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti normative. Il fine è quello di stimolare un continuo miglioramento che consenta a Intesi Group S.p.A. di ridurre al minimo e, ove possibile, eliminare, i rischi di commissione dei reati.

Alla luce di tale finalità, pertanto, tutto il processo di revisione continua (o per adeguamento a modifiche normative o per ristrutturazione aziendale) del Modello Organizzativo permette di ridurre l'entità del rischio in sede di mappatura delle criticità e, conseguentemente, di ottimizzare gli strumenti in uso per la prevenzione del reato.

11. Analisi dei rischi – Approccio e metodo

L'analisi dei rischi è parte cogente e rilevante ai fini di individuare quali elementi, funzioni e/o aree possano considerarsi "sensibili", ovvero nell'ambito delle quali, tenuto conto delle peculiarità della Società, possa configurarsi la commissione di reato (Art. 5 ex D. Lgs. 231/2001).

L'approccio, più funzionale e più proficuo, ai fini della valutazione dei rischi, adottato in Intesi Group S.p.A. è stato quello di identificare ogni processo, mansione e attività in relazione al campo di applicazione / oggetto sociale utilizzando il metodo "Risk Analysis & Management" ("R.A.& M.").

Al fine di effettuare un pieno ed efficace, nonché puntuale R.A.& M. è stata utilizzata una checklist di riscontro per la verifica della conformità legislativa e, in particolare, sono stati presi in considerazione i sotto citati provvedimenti:

- Fonti normative e regolamentari:
  - Codice penale;
  - Codice di procedura penale;
  - Linee Guida Confindustria;
  - D.lgs. 81/2008 s.m.i.;
  - T.U. Ambientale D.lgs. 152/2006 – linee guida gestione ambientale;
  - Regolamento (UE) 679/2016 e D.lgs. 196/2003 privacy & sicurezza dei dati (come modificato dal D.lgs. 101/2018);
  - Dottrina e pronunce rilevanti in ambito D.lgs. 231/2001.
- Fonti interne alla Società da cui si evincono sistemi di controllo già operanti in azienda ed in linea con i principi e le finalità del Decreto:
  - Il Codice di Condotta esprime i principi di "deontologia aziendale" riconosciuti come propri e sui quali la Società richiama l'osservanza da parte di tutti i Dipendenti, Organi Sociali, Consulenti e Partner;
  - procedure aziendali, documentazione e disposizioni inerenti la struttura gerarchico-funzionale ed organizzativa aziendale e sistema di controllo della

gestione. Di tali documenti si è avuto riscontro nel corso delle interviste condotte con le funzioni delle aree rilevanti della Società;

- norme inerenti il sistema amministrativo, contabile, finanziario e di reporting;
- modalità attraverso cui è effettuata la comunicazione interna e la formazione del personale;
- sistema disciplinare di cui ai CCNL (di riferimento).

La metodologia adottata per la predisposizione del Modello prevede di affrontare il problema con una strategia di tipo bottom-up (situazione iniziale –verso obiettivo finale) e consiste in:

- Identificazione delle aree e delle attività “sensibili/rilevanti”;
- Identificazione degli elementi di rischio teorico (aree, attività e reati);
- Valutazione degli elementi in termini di correlazione area/attività/rischio-reato;
- Valutazione dei sistemi di controllo esistenti;
- Sviluppo di piani di adeguamento per i rischi-reato non accettabili.

La metodologia utilizzata è volta a conferire al Modello le caratteristiche di efficacia, specificità e di attualità.

Quanto all’efficacia, si realizza se il Modello è idoneo in concreto a prevenire, o quantomeno ridurre significativamente, il rischio di commissione dei reati previsti dal D.lgs. 231/2001. Tale idoneità è garantita dall’esistenza di meccanismi di decisione e di controllo preventivo e successivo, idonei ad identificare le operazioni che possiedono caratteristiche anomale, a segnalare le condotte rientranti nelle aree di rischio e i conseguenti strumenti di tempestivo intervento. L’efficacia di un Modello organizzativo, infatti, è anche funzione dell'efficienza degli strumenti idonei ad identificare "sintomatologie da illecito".

Quanto alla specificità, si tratta di uno degli elementi che connota l'efficacia del Modello. La specificità del Modello è connessa alle aree a rischio - e impone un censimento delle attività nel cui ambito possono essere commessi i reati – e ai processi di formazione e attuazione delle decisioni dell'ente nelle aree "sensibili”. In tale prospettiva il Modello deve individuare (tra le altre) idonee

modalità di gestione delle risorse finanziarie, prevedere obblighi d'informativa e un adeguato sistema disciplinare oltre che tener conto delle caratteristiche e dimensioni della società, del tipo di attività svolta, nonché della storia della società.

Quanto all'attualità, le caratteristiche di cui sopra (efficacia e specificità) devono essere mantenute nel tempo; pertanto, il Modello è idoneo a ridurre i rischi da reato solo se è costantemente adattato ai caratteri della struttura e dell'attività della Società.

Nel rispetto di quanto sopra indicato con riferimento alla metodologia utilizzata nella redazione del Modello e alle caratteristiche che lo connotano, l'Analisi e Gestione del Rischio è stata elaborata in base alle attività, ai processi, alle responsabilità e ai soggetti/funzioni responsabili presenti alla data di approvazione del presente Modello Organizzativo. L'Analisi e Gestione del Rischio viene periodicamente (ri)effettuata dall'Organismo di Vigilanza ("O.d.V") e comunque riesaminata qualora vi siano variazioni a seguito di eventi rilevanti, quali:

- modifiche al D.lgs. 231/2001 o modifiche normative e/o regolamentari che possono avere un impatto sul Decreto;
- variazioni nella compagine societaria, nell'amministrazione e nelle cariche sociali;
- attribuzione di procure o deleghe a soggetti diversi da quelli a cui erano state attribuite precedentemente;
- variazioni dell'oggetto sociale con l'inserimento di nuove attività;
- cambiamenti aziendali (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, modifiche della struttura organizzativa, ecc.);
- successive valutazioni emerse in sede di riesame del Modello;
- non conformità rilevate dall'O.d.V per un potenziale rischio;
- segnalazioni interne o da parte di terzi (anche da parte di autorità o organismi di vigilanza);
- la percezione di debolezze nei sistemi di controllo adottati.

Analizzati gli ambiti in cui opera la Società ed effettuata la verifica delle aree/funzioni considerate sensibili, in cui può configurarsi la commissione di reato, si è proceduto con la valutazione di rischio di reato tramite la combinazione dei fattori elencati ai successivi paragrafi.

11.1 Probabilità di accadimento

Si tratta della probabilità che un evento illecito accada. Tale fattore è collegato alla FATTIBILITÀ e alla FREQUENZA che un'azione, un processo, un evento, possa manifestarsi come minaccia o come commissione di reato.

Nell'ambito della analisi effettuata si è tenuto conto:

- del rischio potenziale (o assoluto), che si identifica con il rischio insito in una certa attività, senza tener conto del fatto che possono esistere strumenti e protocolli di prevenzione o regolamentazione. Per "rischio" si intende qualsiasi variabile o fattore che nell'ambito dell'azienda, da soli o in correlazione con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi indicati dal Decreto (in particolare all'art. 6, comma 1, lett. a); pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi; e
- del rischio residuo, che si identifica con il rischio che risulta dalla riduzione del rischio potenziale attraverso l'applicazione degli strumenti di prevenzione e controllo già adottati dalla Società. In tale prospettiva si è proceduto alla valutazione del sistema esistente all'interno della Società per la prevenzione dei reati rilevanti ai sensi del Decreto ed il suo eventuale adeguamento in termini di capacità di contrastare efficacemente, cioè ridurre, i rischi identificati. Sotto il profilo concettuale, ridurre un rischio comporta di dover intervenire - congiuntamente o disgiuntamente - su due fattori determinanti: i) la probabilità di accadimento dell'evento e ii) l'impatto dell'evento stesso. In tal senso va interpretato il criterio conservativo che ha improntato la redazione e le valutazioni sottese al presente Modello, intese a

contenere entro il limite fisiologico il rischio. Limite che può identificarsi con il parametro dell'accettabilità3.

Al fine di valutare la FATTIBILITA' si devono considerare gli elementi seguenti.

11.1.1 Vantaggio o interesse economico risultante (dell'ente)

Fattori o criteri per valutare l'aspetto economico4 risultante:	peso / valore
basso rilievo economico per l'ENTE	(1)
alto rilievo economico per l'ENTE	(2)

N.B.: ai soli fini del D.lgs. 231/2001 il reato deve creare un vantaggio o un interesse all'ente.

[3]Nella progettazione di sistemi di controllo a tutela dei rischi di business, definire il rischio accettabile è un'operazione relativamente semplice, almeno dal punto di vista concettuale. Il rischio è ritenuto accettabile quando i controlli aggiuntivi "costano" più della risorsa da proteggere (ad esempio: le comuni automobili sono dotate di antifurto e non anche di un vigilante armato). Nel caso del Decreto la logica economica dei costi non può però essere un riferimento utilizzabile in via esclusiva. È pertanto importante che ai fini dell'applicazione delle norme del Decreto sia definita una soglia effettiva che consenta di porre un limite alla quantità/qualità delle misure di prevenzione da introdurre per evitare la commissione dei reati considerati. In assenza di una previa determinazione del rischio accettabile, la quantità/qualità di controlli preventivi istituibili è, infatti, virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale. Del resto, il generale principio, invocabile anche nel diritto penale, dell'esigibilità concreta del comportamento rappresenta un criterio di riferimento ineliminabile anche se, spesso, appare difficile individuarne in concreto il limite. Riguardo al sistema di controllo preventivo da costruire in relazione al rischio di commissione delle fattispecie di reato contemplate dal Decreto la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente. Questa soluzione è in linea con la logica della "elusione fraudolenta" del modello Organizzativo quale esimente espressa dal D.lgs. 231/2001 ai fini dell'esclusione della responsabilità amministrativa dell'ente (art. 6, comma 1, lett. c, "le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione"). Nel caso dei reati colposi la soglia di rischio accettabile è rappresentata dalla realizzazione di una condotta in violazione del modello Organizzativo di prevenzione (e, nel caso dei reati in materia di salute e sicurezza, dei sottostanti adempimenti obbligatori prescritti dalle norme prevenzionistiche), nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal decreto 231 da parte dell'Organismo di Vigilanza (Tratto dalle Linee Guida di Confindustria del giugno 2021).

[4] Per l'Ente potrebbe essere un maggior ricavo o introito e/o un minor costo o un minor esborso.

11.1.2 Vulnerabilità e presidio

Fattori o criteri per valutare la vulnerabilità ed il controllo del presidio:	peso / valore
L'attività è gestita in autonomia con propria discrezione	(5)
L'attività è gestita in autonomia ma con prescrizioni cogenti e interne	(3)
L'attività è gestita in autonomia con prescrizioni cogenti e interne con controlli e/o monitoraggi continui	(1)
N.B.: i punti (2) e (3) possono avere come controllo finale il benestare (poteri di controllo e di firma in quanto amministratori, o per procura e/o delega)	

Fattori o criteri per valutare la vulnerabilità ed il controllo del presidio:	peso / valore
La presente valutazione deve tener conto dell'incidenza che un fatto "negativo" possa manifestarsi in quanto il processo e/o l'attività non è pienamente gestita da una singola persona, ma attraverso l'intervento di più persone.	
L'attività viene gestita dalla singola persona avente responsabilità	(1)
L'attività gestita non è gestita da una singola persona ma necessita del processo / attività / interventi di una o più persone	(3)

11.1.3 Esperienza, capacità e formazione

Fattori o criteri per valutare la capacità in relazione alla formazione e/o informazione riferita a leggi, responsabilità, prescrizioni interne e in riferimento ai principi del D.lgs. 231/2001:	peso / valore
la persona ha esperienza ed è capace di svolgere la propria attività in relazione alle informazioni in suo possesso / conosce i principi etici, legislativi e le prescrizioni interne	(1)
la persona svolge la propria attività ma necessita di informazioni o formazione sugli aspetti legislativi, sulle prescrizioni interne e sui principi richiamati nel Codice di Condotta	(3)

11.2 Legenda delle probabilità

Calcolo del punteggio emerso dalle tabelle sopra indicate da 4 a 13.

Valore	Livello probabilità
Valore uguale a 4	Remota
Valore da 5 a 6	Poco probabile
Valori da 7 a 10	Probabile
Valori da 11 a 13	Altamente probabile

11.3 Impatto

Si tratta delle conseguenze che un reato possa determinare alla Società in riferimento alla combinazione e/o concomitanza, delle conseguenze economico/finanziarie, interdizioni dell'esercizio delle funzioni, perdita o revoche di autorizzazioni, accreditamenti, licenze, perdita di immagine e altri aspetti negativi che compromettono la Società nelle ordinarie attività economico / gestionali.

Al fine di valutare l'IMPATTO si devono considerare i seguenti elementi:

Sanzioni – impatto economico finanziario	peso / valore
In relazione alle sanzioni previste, l'impatto economico / finanziario, relativamente alle condizioni economiche e alla liquidità dell'ente, può essere:	
Poco rilevante, di non complicata risoluzione	(1)
Rilevante, che influisce sull'andamento economico / finanziario	(3)

Impatto organizzativo/ societario	peso / valore
In relazione alle interdizioni, alla incapacità di esercitare le funzioni (aree, funzioni specifiche interne, amministrazione societaria / figure apicali coinvolte, P.A.), l'impatto può essere:	
"grave" può compromettere l'esercizio economico ma può essere risolvibile	(1)

“altamente grave” compromette l’esercizio economico ed è di difficile e complessa risoluzione	(3)

Immagine/reputazione	peso / valore
La commissione del reato può avere risvolti mediatici più o meno manifesti ed influenti in relazione all’evento o alla gravità del reato:	
Si tratta di un risvolto mediatico di bassa intensità, circoscritto a pochi soggetti	(1)
Si tratta di un risvolto mediatico di bassa intensità, circoscritto territorialmente	(2)
Si tratta di un risvolto mediatico ad ampia diffusione che può compromettere l’esercizio economico	(3)

11.4 Legenda degli impatti

Calcolo del punteggio emerso dalle tabelle sopra indicate da 3 a 9.

Valore	Livello impatto
Valore pari a 3	Basso impatto
Valore pari a 4	Impatto medio

Valori da 5 a 6	Impatto rilevante
Valori da 7 a 9	Grave impatto

Di seguito è rappresentato il valore attribuito all'area / funzione / processo critico in quanto condizione di possible commissione di reato o di potenziale commissione di reato.

		Probabilità			
		REMOTA	POCO PROBABILE	PROBABILE	ALTAMENTE PROBABILE
Impatto	GRAVE IMPATTO	RISCHIO MINORE	RISCHIO MEDIO	RISCHIO ALTO	RISCHIO ALTO
	IMPATTO RILEVANTE	RISCHIO BASSO	RISCHIO MINORE	RISCHIO MEDIO	RISCHIO ALTO

	IMPATTO MEDIO	RISCHIO BASSO	RISCHIO MINORE	RISCHIO MINORE	RISCHIO MEDIO
	IMPATTO BASSO	RISCHIO BASSO	RISCHIO BASSO	RISCHIO BASSO	RISCHIO MINORE

RISCHIO BASSO	I protocolli adottati sono efficaci, necessità del controllo dell'O.d.V.
RISCHIO MINORE	I protocolli esistenti sono funzionali ma sono necessari controlli cadenzati del diretto superiore e dell'O.d.V.
RISCHIO MEDIO	I protocolli devono essere riesaminati per renderli più efficaci ed è necessario un continuo monitoraggio. Qualora necessario, rimuovere gli elementi che possono determinare il potenziale configurarsi del rischio.
RISCHIO ALTO	Sono necessari interventi urgenti per abbattere o minimizzare il rischio di reato.

12. Ambiente generale di controllo

Il sistema di controlli preventivi dovrà essere tale che lo stesso:

- nel caso di reati dolosi, non possa essere aggirato se non fraudolentemente;
- nel caso di reati colposi, incompatibili con il dolo, risulti comunque violato nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito organismo.

Si delineano in particolare i seguenti livelli di presidio:

- un 1° livello di controllo, che definisce e gestisce i controlli cosiddetti di linea, insiti nei processi operativi, e i relativi rischi. È svolto generalmente dalle risorse interne della struttura, sia in autocontrollo da parte dell'operatore, sia da parte del preposto/dirigente ma può comportare, per aspetti specialistici (ad esempio per verifiche strumentali) il ricorso ad altre risorse interne o esterne all'azienda. È bene, altresì, che la verifica delle misure di natura organizzativa e procedurale relative alla salute e sicurezza venga realizzata dai soggetti già definiti in sede di attribuzione delle responsabilità (in genere si tratta di dirigenti e preposti);
- un 2° livello di controllo, svolto da strutture tecniche aziendali competenti in materia e indipendenti da quelle del 1° livello, nonché dal settore di lavoro sottoposto a verifica. Tale monitoraggio presidia il processo di gestione e controllo dei rischi legati all'operatività del sistema, garantendone la coerenza rispetto agli obiettivi aziendali;
- un 3° livello di controllo, effettuato dall'Internal Audit, che fornisce assurance, ovvero valutazioni indipendenti sul disegno e sul funzionamento del complessivo Sistema di Controllo Interno, accompagnato da piani di miglioramento definiti in accordo con il management.

Secondo le indicazioni appena fornite, qui di seguito sono elencate, quelle che generalmente vengono ritenute le componenti di un sistema di controllo preventivo (cd. protocolli) attuate a livello aziendale per garantire l'efficacia del Modello.

12.1 Codice di Condotta

L'adozione di principi etici, ovvero l'individuazione dei valori aziendali primari cui la Società intende conformarsi è espressione di una determinata scelta aziendale e costituisce la base su cui impiantare il sistema di controllo preventivo. Deve costituire profilo di riferimento per ogni realtà imprenditoriale la raccomandazione di un elevato standard di professionalità, nonché il divieto di comportamenti che si pongano in contrasto con le disposizioni legislative e con i valori deontologici.

Principi etici sono contenuti sia nel Codice di Condotta adottato dalla Società, sia, più specificamente nelle singole procedure adottate con riferimento alle singole aree operative.

Segnatamente:

- la Società ha come principio imprescindibile il rispetto di leggi e regolamenti vigenti in tutti i paesi in cui essa opera;
- ogni operazione e transazione deve essere legittima, coerente e congrua, correttamente registrata, autorizzata, verificabile;
- sono previsti principi base relativamente ai rapporti con gli interlocutori della Società;
- vanno adottati principi e criteri in base ai quali vengono prese le decisioni in materia di salute e sicurezza sul lavoro. Principi generali sono contenuti nel Codice di Condotta e specifiche procedure sono adottate dalla funzione competente.

12.2 Il sistema di organizzazione della Società

Il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità e di poteri di rappresentanza, e la definizione delle linee gerarchiche e delle attività operative.

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- conoscibilità all'interno della Società;
- chiara e formale delimitazione dei ruoli e funzioni;
- chiara descrizione delle linee di riporto.

Le procedure interne devono essere redatte nel rispetto dei seguenti principi:

- separazione, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude e il soggetto che lo controlla;

- tracciabilità scritta di ciascun passaggio rilevante del processo;
- adeguatezza del livello di formalizzazione.

Con riferimento ai reati in materia di sicurezza e salute dei lavoratori, è necessaria una struttura organizzativa con compiti e responsabilità definiti formalmente in coerenza con lo schema organizzativo e funzionale dell'impresa. Deve essere prevista un'articolazione di funzioni che assicuri le competenze tecniche adeguate e i poteri necessari per valutare, gestire e controllare il rischio per la salute e la sicurezza dei lavoratori (art. 30, comma 3, D.lgs. n. 81/2008).

Per garantire l'effettivo ed appropriato esercizio di tali funzioni si ricorre all'istituto della delega di funzioni, nel rispetto dei limiti e dei requisiti previsti dagli articoli 16 e 17 del decreto 81 del 2008 ed è necessario che:

- siano esplicitati i compiti della direzione aziendale, dei dirigenti, dei preposti, dei lavoratori, del Responsabile del Servizio di Prevenzione e Protezione, del medico competente e di tutti gli altri soggetti, presenti in azienda e previsti dal decreto 81 del 2008 relativamente alle attività di sicurezza di rispettiva competenza, nonché le connesse responsabilità;
- siano in particolare documentati i compiti del Responsabile del Servizio di Prevenzione e Protezione e degli eventuali addetti allo stesso servizio, del Rappresentante dei Lavoratori per la Sicurezza, degli addetti alla gestione delle emergenze e del medico competente.

Al fine di prevenire illeciti ambientali, l'organizzazione della Società deve invece contemplare procedure operative specifiche per effettuare efficacemente l'attività di gestione dei rischi ambientali che possono concorrere alla commissione dei reati richiamati dall'articolo 25-undecies del Decreto. Tra le misure attuate si è ritenuto necessario:

- monitorare l'attività di valutazione dei rischi ambientali in funzione del quadro normativo e del contesto naturalistico-ambientale sul quale le singole divisions insistono;

- formalizzare opportune disposizioni organizzative al fine di individuare i responsabili del rispetto della normativa ambientale ed i responsabili operativi per la gestione delle tematiche ambientali, alla luce della valutazione dei rischi di cui sopra;
- monitorare le attività di pianificazione e consuntivazione delle spese in campo ambientale, di qualificazione, valutazione e monitoraggio dei fornitori (ad es. i laboratori incaricati della caratterizzazione e classificazione dei rifiuti, dell'esecuzione di prelievi, analisi e monitoraggi ambientali, piuttosto che dei trasportatori, smaltitori, intermediari incaricati della gestione dei rifiuti);
- assicurare l'aggiornamento del Modello alla normativa in materia di reati ambientali.

12.3 Il sistema di deleghe e procure

La delega è l'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. I requisiti essenziali del sistema di deleghe, ai fini di un'efficace prevenzione dei reati, sono i seguenti:

- Il capo funzione responsabile delle aree della Società, nel caso in cui sussista la necessità di delegare tutto o parte dei suoi poteri a propri collaboratori, ha la responsabilità di accertarsi che gli stessi siano dotati di idonea delega scritta;
- la delega deve indicare:
  - delegante (soggetto cui il delegato riporta gerarchicamente);
  - nominativo e compiti del delegato, coerenti con la posizione ricoperta dallo stesso;
  - ambito di applicazione della delega (es. progetto, durata, prodotto, poteri assegnati e limiti ivi inclusi, etc.);
  - eventuale indicazione di soglie di spesa massima, ove applicabile;
  - data di emissione;
  - firma del delegante.

E' opportuno garantire la documentabilità del sistema di deleghe, al fine di rendere agevole una sua eventuale ricostruzione a posteriori.

E' peraltro opportuno prevedere l'applicazione di sanzioni in caso di violazione dei poteri delegati.

La procura è il negozio giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi. I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei reati sono i seguenti:

- la procura può essere conferita a persone fisiche o a persone giuridiche (che agiranno a mezzo di propri procuratori investiti di analoghi poteri);
- le procure generali sono conferite esclusivamente a soggetti dotati di delega interna o di specifico contratto di incarico che descriva i relativi poteri di gestione e, ove necessario, sono accompagnate da apposita comunicazione che fissi l'estensione di poteri di rappresentanza ed eventualmente limiti di spesa;
- una prassi che disciplini modalità e responsabilità per l'aggiornamento tempestivo delle procure, stabilendo i casi in cui le stesse devono essere attribuite, modificate e revocate.

12.4 I rapporti con consulenti/partner/fornitori: principi generali di comportamento

I rapporti con Consulenti/Partner/Fornitori, nell'ambito dei processi sensibili e/o delle attività a rischio reato devono essere improntati alla massima correttezza e trasparenza, al rispetto delle norme di legge, del Codice di Condotta, del presente Modello e delle procedure aziendali interne, nonché degli specifici principi etici su cui è impostata l'attività della Società.

I consulenti, i fornitori di prodotti/servizi e in generale i partner (es. associazione temporanea d'impresa) devono essere selezionati in considerazione di quanto di seguito specificato:

- verificare l'attendibilità commerciale e professionale (ad es. attraverso visure ordinarie presso la Camera di Commercio per accertare la coerenza dell'attività svolta con le prestazioni richieste dalla Società, autocertificazione ai sensi del D.P.R. 445/00 relativa ad eventuali carichi pendenti o sentenze emesse nei loro confronti);

- selezionare in base alla capacità di offerta in termini di qualità, innovazione, costi e standard di sostenibilità, con particolare riferimento al rispetto dei diritti umani e dei diritti dei lavoratori, dell'ambiente, ai principi di legalità, trasparenza e correttezza negli affari (tale processo di accreditamento deve prevedere standard qualitativi elevati riscontrabili anche mediante l'acquisizione di specifiche certificazioni in tema di qualità da parte di un competente e riconosciuto ente certificatore);
- evitare/non intraprendere rapporti contrattuali con soggetti - persone fisiche o persone giuridiche - che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati non conformi agli standard delle leggi internazionali ed alle raccomandazioni espresse dal FATF-GAFI (Gruppo di Azione Finanziaria contro il riciclaggio di denaro) o che siano riportati nelle liste di prescrizione (cosiddette "Black List") della World Bank e della Commissione Europea. In proposito rilevano anche le c.d. white list previste dalla legge n. 190/2012 e disciplinate dal DPCM del 18 aprile 2013, entrato in vigore il 14 agosto 2013. In attuazione di questa disciplina, presso le Prefetture è stato istituto l'elenco dei fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativo di infiltrazione mafiosa, operanti nei settori esposti maggiormente a rischio (cosiddetta "White List")5. L'iscrizione nell'elenco, che è di natura volontaria, soddisfa i requisiti per l'informazione antimafia per l'esercizio dell'attività per cui è stata disposta l'iscrizione ed è valida per dodici mesi, salvi gli esiti delle verifiche periodiche.

Nell'ambito della gestione dei rapporti con fornitori/clienti/partner/intermediari si precisano inoltre i seguenti principi comportamentali (in relazione al reato di "Corruzione tra privati"):

- non distribuire omaggi e regalie al di fuori di quanto previsto dalla prassi aziendale: gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore ovvero

[5]Le attività imprenditoriali iscrivibili nell'elenco prefettizio sono espressamente individuate nell'art. 1, co. 53 della legge n. 190/2012 come modificata tempo per tempo.

perché volti a promuovere iniziative di carattere benefico o culturale o la brand image della Società. In particolare, è vietata qualsiasi regalia a fornitori/clienti/partner/intermediari che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;

- non effettuare donazioni per beneficenza e sponsorizzazioni senza preventiva autorizzazione o al di fuori di quanto previsto dalla prassi aziendale; tali contributi devono essere destinati esclusivamente a promuovere iniziative di carattere benefico o culturale o la brand image della Società;
- non effettuare spese per pasti, intrattenimento o altre forme di ospitalità al di fuori di quanto previsto dalle prassi aziendale;
- evitare situazioni di conflitto di interesse, con particolare riferimento a interessi di natura personale, finanziaria o familiare (ad es., l'esistenza di partecipazioni finanziarie o commerciali in aziende fornitrici, clienti o concorrenti, vantaggi impropri derivanti dal ruolo svolto all'interno della Società, ecc.), che potrebbero influenzare l'indipendenza verso fornitori/clienti/partner/intermediari;
- non effettuare elargizioni in denaro e non accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) a fornitori/clienti/partner sia direttamente sia tramite intermediari;
- non riconoscere compensi, commissioni, offrire o promettere vantaggi di qualsiasi natura a fornitori/clienti/partner/intermediari che non trovino adeguata giustificazione nel contesto del rapporto di lavoro o del rapporto contrattuale costituito con gli stessi e alle prassi vigenti in ambito locale;
- non assumere o fare promesse di assunzione che non siano basate su criteri di oggettività, competenza e professionalità e che non siano adeguatamente documentate;
- prevedere adeguate segregazioni di compiti e responsabilità nella gestione:

  - del fornitore/partner/intermediario, con particolare riferimento alla valutazione delle offerte, all'esecuzione della prestazione/fornitura e al suo benestare, nonché alla liquidazione dei pagamenti;
  - del cliente, con particolare riferimento alla definizione del prezzo, delle condizioni e tempi di pagamento e alla scontistica;
- qualunque transazione finanziaria deve presupporre la conoscenza del beneficiario della relativa somma;
- nessun pagamento può essere effettuato in contanti e nel caso di deroga gli stessi pagamenti dovranno essere opportunamente autorizzati. In ogni caso i pagamenti devono essere effettuati nell'ambito di apposite procedure amministrative, che ne documentino la riferibilità e la tracciabilità della spesa;
- verificare la coerenza tra l'oggetto del contratto e la prestazione/fornitura effettuata, nonché la coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- investigare con attenzione e segnalare all'Organismo di Vigilanza:
  - richieste di effettuare pagamenti a una terza parte anziché direttamente all'agente o rappresentante;
  - richieste di commissioni insolitamente elevate;
  - richieste di rimborsi spese non adeguatamente documentate ovvero insolite per l'operazione in questione;
  - concessione di sconti discrezionali non adeguatamente documentati;
  - richieste di effettuare pagamenti da/verso un conto diverso da quello indicato nell'anagrafica o relativo ad istituti di credito aventi sede in paradisi fiscali o che non hanno insediamenti fisici in alcun Paese.

Con riferimento alla gestione finanziaria, la Società attua specifici controlli procedurali e cura con particolare attenzione i flussi che non rientrano nei processi tipici dell'azienda e che sono quindi gestiti in modo estemporaneo e discrezionale. Tali controlli (ad es. l'attività di frequente riconciliazione dei dati contabili, la supervisione, la separazione dei compiti, la contrapposizione

delle funzioni, in particolare quella acquisti e quella finanziaria, un efficace apparato di documentazione del processo decisionale, ecc.) hanno lo scopo di impedire la formazione di riserve occulte.

L'osservanza dei principi sopra riportati è rilevante anche nell'ottica di evitare che si creino situazioni che possono agevolare la commissione di reati in concorso. Infatti, la responsabilità della Società può sussistere anche laddove il dipendente autore dell'illecito abbia concorso nella sua realizzazione con soggetti estranei all'organizzazione della Società medesima. Tale ipotesi è chiaramente rappresentata nel Codice penale e, in particolare, negli artt. 110 c.p.[6] e 113 c.p.[7] . Risulta, invece, non altrettanto immediata la sua rilevanza ai fini del decreto 231. Diversi possono essere i settori di business nei quali può annidarsi più facilmente il rischio del coinvolgimento in concorso del dipendente e quindi, ricorrendone i presupposti di interesse e/o vantaggio, dell'ente.

12.5 I rapporti con consulenti/partner/fornitori: clausole contrattuali

I contratti con consulenti/partner/fornitori devono prevedere la formalizzazione di apposite clausole che:

- regolano l'impegno al rispetto del Codice di Condotta e del Modello adottati da Intesi Group S.p.A., nonché la dichiarazione di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Modello della Società stessa e nel D. Lgs. 231/2001 (o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte della Società in caso si addivenga all'instaurazione del

[6] "Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita."

[7] "Nel delitto colposo, quando l'evento è stato cagionato dalla cooperazione di più persone, ciascuna di queste soggiace alle pene stabilite per il delitto stesso.

rapporto di consulenza o partnership). Tale impegno potrà esser reciproco, nel caso in cui la controparte abbia adottato un proprio e analogo Codice di Condotta e Modello;

- definiscono le conseguenze della violazione delle norme di cui al Modello e/o al Codice di Condotta (es. clausole risolutive espresse, penali);
- regolano l'impegno di consulenti/partner stranieri, a condurre la propria attività in conformità a regole e principi analoghi a quelli previsti dalle leggi dello Stato (o degli Stati) ove gli stessi operano, con particolare riferimento ai reati di corruzione, riciclaggio e terrorismo e alle norme che prevedono una responsabilità per la persona giuridica (Corporate Liability), nonché ai principi contenuti nel Codice di Condotta, finalizzati ad assicurare il rispetto di adeguati livelli di etica nell'esercizio delle proprie attività;
- consentono alla Società o a persone/enti delegati dalla stessa, in coerenza con la tipologia dei contratti, di effettuare ispezioni, verifiche e controlli concernenti l'adempimento sulle attività oggetto di contratto nonché di prevedere operazioni di collaudo finale sul bene acquistato.

12.6 I rapporti con clienti: principi generali di comportamento

I rapporti con i clienti devono essere improntati alla massima correttezza e trasparenza, nel rispetto del Codice di Condotta, del presente Modello, delle norme di legge e delle procedure aziendali interne, che prendono in considerazione gli elementi qui di seguito indicati a titolo esemplificativo:

- accettare pagamenti in contanti (e/o altra modalità non tracciate) solo nei limiti consentiti dalla legge e previa autorizzazione scritta;
- concedere dilazioni di pagamento solamente a fronte di accertata solvibilità;
- rifiutare le vendite in violazioni a leggi/regolamenti internazionali, che limitano l'esportazione di prodotti/servizi e/o tutelano i principi della libera concorrenza;

- praticare prezzi in linea con i valori medi di mercato, fatte salve le promozioni commerciali e le eventuali donazioni, a condizione che entrambe siano adeguatamente motivate/autorizzate;
- la fase di individuazione delle opportunità commerciali sia improntata a criteri di correttezza e trasparenza.

12.7 Sistema di gestione dei flussi finanziari

La Società adotta un sistema di gestione dei flussi finanziari improntato ai principi di trasparenza, verificabilità e inerenza all'attività aziendale, utilizzando meccanismi di procedimentalizzazione delle decisioni che consentono di documentare e verificare le varie fasi del processo decisionale, al fine di impedire la gestione impropria delle risorse della Società.

Una corretta gestione del processo, anche secondo quanto dispone l'art. 6, comma 2, lett. c) del D.lgs. 231/2001, contribuisce a prevenire il rischio di commissione di molteplici reati da parte della Società.

Relativamente alla gestione dei flussi finanziari la Società applica i seguenti principi di controllo:

- separazione dei compiti nelle fasi/attività chiave del processo (es. autorizzazione, riconciliazione);
- sistema di deleghe e procure costantemente allineato con i profili autorizzativi residenti sui sistemi informativi;
- sistema di prassi/procedure interne che regolamentano i principali processi su cui impattano i flussi finanziari;
- adeguata tracciabilità dei flussi informativi e documentali.

In particolare, la Società ha adottato prassi/procedure che regolamentano le attività inerenti alla gestione dei flussi finanziari, con specifico riferimento alle attività di predisposizione del bilancio, nonché di autorizzazione e valutazione delle iniziative di investimento.

12.8 Sistemi informativi

Devono essere tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo.

Una particolare efficacia preventiva riveste lo strumento di controllo rappresentato dalla separazione di compiti fra coloro che svolgono fasi o attività cruciali di un processo a rischio.

In questo campo, specifico interesse ricopre l'area della gestione finanziaria, dove il controllo procedurale si avvale di strumenti consolidati nella pratica amministrativa, quali per esempio abbinamento firme, riconciliazioni frequenti, supervisione, separazione di compiti con la già citata contrapposizione di funzioni, ad esempio fra la funzione acquisti e quella finanziaria.

Particolare attenzione deve essere riposta sui flussi finanziari non rientranti nei processi tipici aziendali, soprattutto se si tratta di ambiti non adeguatamente proceduralizzati e con caratteri di estemporaneità e discrezionalità.

In ogni caso è necessario che siano sempre salvaguardati i principi di trasparenza, verificabilità, inerenza all'attività aziendale. Sarà opportuno valutare nel tempo la separazione dei compiti all'interno di ogni processo a rischio, verificando che le procedure aziendali e/o le prassi operative siano periodicamente aggiornate e tengano costantemente in considerazione le variazioni o novità intervenute nei processi aziendali e nel sistema organizzativo.

12.9 Comunicazione al personale e sua formazione

Sono due importanti requisiti del modello ai fini del suo buon funzionamento e devono essere diversamente modulati in base ai destinatari: i dipendenti nella loro generalità, quelli che operano in specifiche aree di rischio/attività sensibili, i componenti degli organi sociali ecc.

Con riferimento alla comunicazione, essa deve riguardare ovviamente il Codice di Condotta, il Modello, ma anche gli altri strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazione. La comunicazione deve essere: capillare, efficace, autorevole

(cioè emessa da un livello adeguato), chiara e dettagliata, periodicamente ripetuta. Inoltre, è previsto l'accesso e la consultazione della documentazione costituente il Modello anche attraverso l'intranet aziendale.

Accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione modulato in funzione dei livelli dei destinatari.

È importante che l'attività di formazione sul Decreto e sui contenuti del Modello sia promossa e supervisionata dall'Organismo di Vigilanza della Società.

13. Divieti di carattere generale

Al fine di evitare la commissione dei reati sopra elencati, è sempre ed espressamente vietato porre in essere le condotte di seguito elencate a titolo esemplificativo:

- adottare comportamenti che costituiscano un reato o che comunque siano in violazione di legge e/o di regolamenti;
- usare la propria posizione per ottenere benefici o privilegi per sé o per altri;
- corrispondere od offrire, direttamente o indirettamente, pagamenti o benefici materiali a pubblici ufficiali o incaricati di pubblico servizio per influenzare o compensare un atto del loro ufficio (o ad esso contrario) ed assicurare vantaggi di qualunque tipo alla Società;
- utilizzare lo strumento dell'assunzione o il sistema retributivo per accordare vantaggi diretti o indiretti a pubblici ufficiali o incaricati di pubblico servizio;
- presentare dichiarazioni non veritiere a organismi pubblici;
- offrire o promettere denaro, doni o altre liberalità, direttamente o indirettamente al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, ai rappresentanti della PA o a loro familiari non deve essere offerta, né

direttamente né indirettamente, qualsiasi forma di regalo, doni o gratuite prestazioni che possano apparire, comunque, connessi al rapporto di affari con la Società o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società;

- destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi, o finanziamenti, a scopi diversi da quelli per cui sono state concesse;
- emettere richieste di acquisto che non trovino riscontro in una specifica e motivabile esigenza della Società e che non siano autorizzate in base alle deleghe conferite;
- riconoscere compensi a consulenti e fornitori che non trovino giustificazione in relazione al tipo di incarico da svolgere ed ai prezzi di mercato;
- effettuare pagamenti con mezzi non tracciabili o su conti cifrati;
- emettere assegni bancari senza clausola di non trasferibilità;
- utilizzare le risorse informatiche della Società per fini diversi da quelli connessi allo svolgimento delle attività proprie dell'impresa;
- favorire l'ingresso o la permanenza nello Stato di soggetti non aventi diritto;
- intrattenere rapporti economici o commerciali con soggetti od enti che risultino essere direttamente o indirettamente coinvolti in associazioni terroristiche od eversive.

Con particolare riferimento ai reati societari richiamati dall'art. 25 ter D.lgs. 231/01 (reati societari) è espressamente vietato (tra l'altro):

- elaborare o comunicare dati falsi o tali da fornire una descrizione scorretta della situazione economica, patrimoniale e finanziaria della Società;
- omettere di comunicare informazioni previste dalla normativa vigente o dalle regole interne, relativamente alla situazione economica, patrimoniale e finanziaria della Società;
- ripartire utili o acconti non effettivamente conseguiti o da destinarsi per legge a riserva o comunque in violazione delle norme statutarie;

- ripartire riserve nei casi in cui ciò non è consentito dalla legge;
- ridurre il capitale sociale od effettuare fusioni o scissioni violando le disposizioni di legge a tutela dei creditori;
- formare o aumentare in modo fittizio il capitale sociale;
- realizzare o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con la Società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse di Intesi Group S.p.A. e nel pieno rispetto delle norme del Codice di Condotta;
- porre in essere atti tali da alterare la regolare formazione della volontà dell'assemblea e fornire all'assemblea dei soci stessa, informazioni non veritiere o alterate nei loro contenuti.

14. Le fattispecie di reato richiamate dal D.lgs. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati dall'art. 5 del D. Lgs. 231/2001 è collegato il regime di responsabilità a carico della Società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal Decreto Legislativo.

A tal fine, si riportano i reati richiamati nel D.lgs. 231/2001 rilevanti per la Società (dettagliati nell'allegato unitamente alle sanzioni):

Le fattispecie di reato ex D.lgs. 231/2001	**Applicabilità**
art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche	Sì

Le fattispecie di reato ex D.lgs. 231/2001	Applicabilità
forniture	
art. 24-bis - Delitti informatici e trattamento illecito di dati	Sì
art. 24-ter - Delitti di Criminalità Organizzata	Sì
art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio	Sì
art. 25-bis - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento	Sì
art. 25-bis1 - Delitti contro l'Industria e il Commercio	Sì
art. 25-ter - Reati societari, inclusa la corruzione tra privati	Sì
art. 25-quater - Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali	No
art. 25-quater.1 - Pratiche di mutilazione degli organi genitali femminili	No
art. 25-quinquies - Delitti contro la personalità individuale	Sì
art. 25-sexies - Abusi di mercato	Sì

Le fattispecie di reato ex D.lgs. 231/2001	Applicabilità
art. 25-septies - Omicidio colposo e lesioni colpose gravi o gravissime, commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	Sì
art. 25-octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché auto riciclaggio	Sì
art. 25 octies 1 - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	Sì
art. 25-novies - Delitti in materia di violazione del Diritto di Autore	Sì
art. 25-decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Sì
art. 25-undecies - Reati ambientali	Sì
art. 25-duodecies - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Sì
art. 25-terdecies - Razzismo e Xenofobia	No
art. 25-quaterdecies - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a	No

Le fattispecie di reato ex D.lgs. 231/2001	Applicabilità
mezzo di apparecchi vietati	
art. 25- quinquesdecies - Reati tributari	Sì
art. 25-sexiesdecies - Contrabbando	Sì
Art. 25-septiesdecies - Delitti contro il patrimonio culturale	No
Art. 25-octiesdecies – Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici	No
L. n. 146/2006 - Reati transnazionali	Sì

15. Le attività sensibili ai fini del D.lgs. 231/2001

L'art. 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001.

L'analisi svolta nel corso del progetto di revisione, ha permesso di individuare le aree di Intesi Group S.p.A. nell'ambito delle quali sono svolte le attività che possono essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dal D. Lgs. 231/2001.

Le aree in cui le attività "sensibili" sopraelencate sono esercitate sono:

- Amministrazione e Finanza
- Tax
- Processo di gestione contanti e carte di credito/debito aziendali
- Selezione, assunzione e gestione delle risorse umane
- Tutela e sicurezza sul lavoro
- Tutela ambiente
- Gestione commerciale
- Processo gestione acquisti
- Gestione sistema informatico – Sicurezza dei dati
- Procedimenti giudiziari ed arbitrali
- Rapporti con la Pubblica Amministrazione
- Gestione della Società per opera degli organi amministrativi e di controllo
- Gestione informazioni privilegiate e informativa pubblica
- Processi per la partecipazione a gare d'appalto pubbliche e private.

Propedeutica all'individuazione delle aree/attività sensibili è stata l'analisi della struttura ed organizzazione della Società, svolta al fine di meglio comprendere l'attività della stessa e di identificare (i) gli ambiti aziendali oggetto dell'intervento e (ii) le funzioni responsabili di tali aree ossia, le persone di più alto livello organizzativo in grado di fornire le informazioni di dettaglio sui singoli processi aziendali e sulle attività delle singole funzioni in quanto provviste di una conoscenza approfondita dei processi/attività sensibili e dei meccanismi di controllo attualmente in essere.

La raccolta della documentazione rilevante ai fini del Modello (es. procedure) e la verifica della stessa con il supporto delle funzioni responsabili delle aree rilevanti della Società (tramite interviste condotte ad hoc) ha permesso la individuazione dei processi/attività sensibili.

16. Il sistema dei controlli

I protocolli di controllo sono edificati sui seguenti principi generali, i quali devono essere rispettati nell'ambito di ogni attività sensibile individuata:

- Regolamentazione: esistenza di regole formali o prassi consolidate, di procedure ed istruzioni operative idonee a fornire linee di condotta e modalità operative adeguate allo svolgimento delle attività, anche sensibili;
- Segregazione dei compiti: separatezza delle funzioni operative dalle funzioni di controllo
- Tracciabilità: principio secondo il quale:
  - ogni operazione relativa all'attività sensibile deve essere, ove possibile, opportunamente registrata;
  - il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali.
- Poteri autorizzativi e di firma: i poteri autorizzativi e di firma devono essere:
  - coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese;
  - chiaramente definiti e conosciuti all'interno di Intesi Group S.p.A.

Oltre ai sopra elencati principi generali, in relazione alle singole attività, sono indicati protocolli di controllo specifici, volti a mitigare rischi tipici del processo sensibile considerato.

Al fine di rilevare ed analizzare in dettaglio il sistema di controllo interno esistente a presidio dei rischi riscontrati ed evidenziati nell'attività di risk assessment sopra descritta e di valutare la conformità del Modello stesso alle previsioni del D.lgs. 231/01, è stata effettuata un'analisi

comparativa (la c.d. “gap analysis”) tra il Modello di organizzazione, gestione e controllo esistente (“as is”) e un Modello astratto di riferimento valutato sulla base delle esigenze manifestate dalla disciplina di cui al D.lgs. 231/01 (“to be”).

17. Descrizione schema tabelle

Di seguito vengono identificate le aree (funzioni, attività e processi) ritenute sensibili o critiche secondo seguente schema:

- aree (funzioni, attività e processi)
- le fattispecie di reato rilevanti per singola area
- i fattori di rischio
- parti interessate coinvolte:
  - funzioni apicali
  - collaboratori interni
  - collaboratori esterni
- principi specifici di comportamento
- presidi di controllo e di monitoraggio:
  - descrizione
  - funzioni (autorità responsabilità)
  - i protocolli attuati